

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2002年 7月10日

出 願 番 号
Application Number:

特願2002-201472

[ST.10/C]:

[JP2002-201472]

出 願 人
Applicant(s):

ソニー株式会社

2003年 6月 2日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3042455

【書類名】 特許願
【整理番号】 0290427104
【提出日】 平成14年 7月10日
【あて先】 特許庁長官 殿
【国際特許分類】 G06F 15/00
H04L 9/32

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 松山 科子

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100110434

【弁理士】

【氏名又は名称】 佐藤 勝

【手数料の表示】

【予納台帳番号】 076186

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0011610

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 リモートアクセスシステム、リモートアクセス方法、リモートアクセスプログラム及びリモートアクセスプログラムが記録された記録媒体

【特許請求の範囲】

【請求項 1】 所定のリソースに対して遠隔地からアクセスするリモートアクセスシステムであって、

アクセスの対象となる上記リソース自体としての機器、又は上記リソースを保持する機器であるアクセス対象機器と、

上記アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入りに相当する機器であるゲートウェイ機器と、

少なくとも上記リソースに対する権限が記述された電子証明書であり、且つ、この電子証明書を経由させる上記ゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持し、上記アクセス対象機器に対してアクセスするアクセス機器とを備え、

上記アクセス機器は、上記権限及び経由情報記述属性証明書を上記ゲートウェイ機器に対して送信して提示し、

上記ゲートウェイ機器は、上記アクセス機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記アクセス対象機器に対して送信して提示し、

上記アクセス対象機器は、上記ゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とするリモートアクセスシステム。

【請求項 2】 上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の提出者が当該権限及び経由情報記述属性証明書の所有者以外である場合に利用され、当該権限及び経由情報記述属性証明書を提出することができるエンティティを示すプロキシ情報として、当該権限及び経由情報記述属性証明書を経由させる上記ゲートウェイ機器の情報が記述されたものであること

を特徴とする請求項 1 記載のリモートアクセスシステム。

【請求項 3】 上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の検証者たる上記アクセス対象機器が当該権限及び経由情報記述属性証明書の所有者を認証する場合に利用するサービスに関する認証情報として、上記リソースに対する権限が記述されたものであること

を特徴とする請求項 1 記載のリモートアクセスシステム。

【請求項 4】 上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の所有者のアクセス許可情報として、上記リソースに対する権限が記述されたものであること

を特徴とする請求項 1 記載のリモートアクセスシステム。

【請求項 5】 上記アクセス機器に対して上記権限及び経由情報記述属性証明書を発行する許可を与えるための電子証明書である発行許可情報記述属性証明書を発行する所定の属性認証局を備え、

上記ゲートウェイ機器は、上記属性認証局によって発行された上記発行許可情報記述属性証明書に基づいて、上記権限及び経由情報記述属性証明書を上記アクセス機器に対して発行すること

を特徴とする請求項 1 記載のリモートアクセスシステム。

【請求項 6】 上記発行許可情報記述属性証明書は、当該発行許可情報記述属性証明書の所有者たる上記ゲートウェイ機器に与えられる役割を示すロール情報として、上記アクセス機器に対して上記権限及び経由情報記述属性証明書を発行する許可を与える旨を示す情報が記述されたものであること

を特徴とする請求項 5 記載のリモートアクセスシステム。

【請求項 7】 公開鍵暗号方式における独立した所定の第三者機関であり電子証明書としての公開鍵証明書を発行する証明書発行認証局を備え、

上記属性認証局は、上記証明書発行認証局とは異なるローカルな機関であること

を特徴とする請求項 5 記載のリモートアクセスシステム。

【請求項 8】 上記証明書発行認証局は、上記アクセス対象機器、上記ゲートウェイ機器、及び上記アクセス機器のそれぞれに対して上記公開鍵証明書を発行

すること

を特徴とする請求項 7 記載のリモートアクセスシステム。

【請求項 9】 上記権限及び経由情報記述属性証明書は、上記アクセス対象機器が属するネットワークとは異なる他のネットワークに属するエンティティによって発行されたものであること

を特徴とする請求項 1 記載のリモートアクセスシステム。

【請求項 10】 上記アクセス対象機器が属するネットワークとは異なる他のネットワークに属する他のアクセス対象機器と、

上記他のネットワークの入り口に相当する機器である他のゲートウェイ機器と、

上記ゲートウェイ機器がアクセスすることができる上記他のネットワークにおけるエンティティとしての上記他のゲートウェイ機器を示す情報が記述された電子証明書であるゲートウェイ機器情報記述属性証明書を発行する所定の属性認証局とを備え、

上記ゲートウェイ機器は、上記属性認証局によって発行された上記ゲートウェイ機器情報記述属性証明書を上記他のゲートウェイ機器に対して送信して提示し、上記権限及び経由情報記述属性証明書を発行してもらい、上記権限及び経由情報記述属性証明書を上記アクセス機器に対して送信すること

を特徴とする請求項 9 記載のリモートアクセスシステム。

【請求項 11】 上記アクセス機器は、上記権限及び経由情報記述属性証明書を上記ゲートウェイ機器に対して送信して提示し、

上記ゲートウェイ機器は、上記アクセス機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記他のアクセス対象機器が属する上記他のネットワークにおける上記他のゲートウェイ機器に対して送信して提示し、

上記他のゲートウェイ機器は、上記ゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記他のアクセス対象機器に対して送信して提示し、

上記他のアクセス対象機器は、上記他のゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とする請求項 1 0 記載のリモートアクセスシステム。

【請求項 1 2】 上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の提出者が当該権限及び経由情報記述属性証明書の所有者以外である場合に利用され、当該権限及び経由情報記述属性証明書を提出することができるエンティティを示すプロシキ情報として、当該権限及び経由情報記述属性証明書を経由させる上記ゲートウェイ機器及び上記他のゲートウェイ機器の両方の情報が記述されたものであること

を特徴とする請求項 1 0 記載のリモートアクセスシステム。

【請求項 1 3】 上記ゲートウェイ機器情報記述属性証明書は、当該ゲートウェイ機器情報記述属性証明書の所有者のアクセス許可情報として、上記ゲートウェイ機器がアクセスすることができる上記他のゲートウェイ機器を示す情報が記述されたものであること

を特徴とする請求項 1 0 記載のリモートアクセスシステム。

【請求項 1 4】 公開鍵暗号方式における独立した所定の第三者機関であり電子証明書としての公開鍵証明書を発行する証明書発行認証局を備え、

上記属性認証局は、上記証明書発行認証局とは異なるローカルな機関であること

を特徴とする請求項 1 0 記載のリモートアクセスシステム。

【請求項 1 5】 上記証明書発行認証局は、上記アクセス対象機器、上記ゲートウェイ機器、上記アクセス機器、上記他のアクセス対象機器、及び上記他のゲートウェイ機器のそれぞれに対して上記公開鍵証明書を発行すること

を特徴とする請求項 1 4 記載のリモートアクセスシステム。

【請求項 1 6】 所定のリソースに対して遠隔地からアクセスするリモートアクセス方法であって、

アクセスの対象となる上記リソース自体としての機器、又は上記リソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少な

くとも上記リソースに対する権限が記述された電子証明書であり、且つ、上記アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を經由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持させ、

上記アクセス機器によって上記権限及び経由情報記述属性証明書を上記ゲートウェイ機器に対して送信して提示し、

上記ゲートウェイ機器によって上記アクセス機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記アクセス対象機器に対して送信して提示し、

上記アクセス対象機器によって上記ゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とするリモートアクセス方法。

【請求項 1 7】 上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の提出者が当該権限及び経由情報記述属性証明書の所有者以外である場合に利用され、当該権限及び経由情報記述属性証明書を提出することができるエンティティを示すプロシキ情報として、当該権限及び経由情報記述属性証明書を經由させる上記ゲートウェイ機器の情報が記述されたものであることを特徴とする請求項 1 6 記載のリモートアクセス方法。

【請求項 1 8】 上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の検証者たる上記アクセス対象機器が当該権限及び経由情報記述属性証明書の所有者を認証する場合に利用するサービスに関する認証情報として、上記リソースに対する権限が記述されたものであること

を特徴とする請求項 1 6 記載のリモートアクセス方法。

【請求項 1 9】 上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の所有者のアクセス許可情報として、上記リソースに対する権限が記述されたものであること

を特徴とする請求項 1 6 記載のリモートアクセス方法。

【請求項 2 0】 所定の属性認証局によって発行された電子証明書であり、上記アクセス機器に対して上記権限及び経由情報記述属性証明書を発行する許可を与えるための電子証明書である発行許可情報記述属性証明書に基づいて、上記ゲートウェイ機器によって上記権限及び経由情報記述属性証明書を上記アクセス機器に対して発行すること

を特徴とする請求項 1 6 記載のリモートアクセス方法。

【請求項 2 1】 上記発行許可情報記述属性証明書は、当該発行許可情報記述属性証明書の所有者たる上記ゲートウェイ機器に与えられる役割を示すロール情報として、上記アクセス機器に対して上記権限及び経由情報記述属性証明書を発行する許可を与える旨を示す情報が記述されたものであること

を特徴とする請求項 2 0 記載のリモートアクセス方法。

【請求項 2 2】 上記属性認証局は、公開鍵暗号方式における独立した所定の第三者機関であり電子証明書としての公開鍵証明書を発行する証明書発行認証局とは異なるローカルな機関とされること

を特徴とする請求項 2 0 記載のリモートアクセス方法。

【請求項 2 3】 上記アクセス対象機器、上記ゲートウェイ機器、及び上記アクセス機器のそれぞれに対して、上記証明書発行認証局によって上記公開鍵証明書を発行すること

を特徴とする請求項 2 2 記載のリモートアクセス方法。

【請求項 2 4】 上記権限及び経由情報記述属性証明書は、上記アクセス対象機器が属するネットワークとは異なる他のネットワークに属するエンティティによって発行されたものであること

を特徴とする請求項 1 6 記載のリモートアクセス方法。

【請求項 2 5】 所定の属性認証局によって発行された電子証明書であり、上記アクセス対象機器が属するネットワークとは異なる他のネットワークにおける上記ゲートウェイ機器がアクセスすることができるエンティティとしての当該他のネットワークの入り口に相当する機器である他のゲートウェイ機器を示す情報が記述されたゲートウェイ機器情報記述属性証明書を、上記ゲートウェイ機器に

よって上記他のゲートウェイ機器に対して送信して提示し、上記権限及び経由情報記述属性証明書を発行してもらい、上記権限及び経由情報記述属性証明書を上記アクセス機器に対して送信すること

を特徴とする請求項 2 4 記載のリモートアクセス方法。

【請求項 2 6】 上記アクセス機器によって上記権限及び経由情報記述属性証明書を上記ゲートウェイ機器に対して送信して提示し、

上記ゲートウェイ機器によって上記アクセス機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書を、アクセスの対象として指定された上記他のネットワークに属する他のアクセス対象機器が属する当該他のネットワークにおける上記他のゲートウェイ機器に対して送信して提示し、

上記他のゲートウェイ機器によって上記ゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定された上記他のアクセス対象機器に対して送信して提示し、

上記他のアクセス対象機器によって上記他のゲートウェイ機器から受信した上記権限及び経由情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とする請求項 2 5 記載のリモートアクセス方法。

【請求項 2 7】 上記権限及び経由情報記述属性証明書は、当該権限及び経由情報記述属性証明書の提出者が当該権限及び経由情報記述属性証明書の所有者以外である場合に利用され、当該権限及び経由情報記述属性証明書を提出することができるエンティティを示すプロシキ情報として、当該権限及び経由情報記述属性証明書を經由させる上記ゲートウェイ機器及び上記他のゲートウェイ機器の両方の情報が記述されたものであること

を特徴とする請求項 2 5 記載のリモートアクセス方法。

【請求項 2 8】 上記ゲートウェイ機器情報記述属性証明書は、当該ゲートウェイ機器情報記述属性証明書の所有者のアクセス許可情報として、上記ゲートウェイ機器がアクセスすることができる上記他のゲートウェイ機器を示す情報が記

述されたものであること

を特徴とする請求項 2 5 記載のリモートアクセス方法。

【請求項 2 9】 上記属性認証局は、公開鍵暗号方式における独立した所定の第三者機関であり電子証明書としての公開鍵証明書を発行する証明書発行認証局とは異なるローカルな機関とされること

を特徴とする請求項 2 5 記載のリモートアクセス方法。

【請求項 3 0】 上記アクセス対象機器、上記ゲートウェイ機器、上記アクセス機器、上記他のアクセス対象機器、及び上記他のゲートウェイ機器のそれぞれに対して、上記証明書発行認証局によって上記公開鍵証明書を発行すること

を特徴とする請求項 2 9 記載のリモートアクセス方法。

【請求項 3 1】 所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なりモートアクセスプログラムであって、

アクセスの対象となる上記リソース自体としての機器、又は上記リソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくとも上記リソースに対する権限が記述された電子証明書であり、且つ、上記アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経路情報記述属性証明書が保持されており、

上記アクセス機器から上記ゲートウェイ機器を介して送信されて提示された上記権限及び経路情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とするリモートアクセスプログラム。

【請求項 3 2】 所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なりモートアクセスプログラムが記録された記録媒体であって、

アクセスの対象となる上記リソース自体としての機器、又は上記リソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくとも上記リソースに対する権限が記述された電子証明書であり、且つ、上記アクセス対象機器が属するネットワークと他のネットワークとを相互に接続するこ

とを可能とするネットワークの入りに相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経路情報記述属性証明書が保持されており、

上記リモートアクセスプログラムは、

上記アクセス機器から上記ゲートウェイ機器を介して送信されて提示された上記権限及び経路情報記述属性証明書の内容を検証し、上記リソースに対する上記アクセス機器のアクセスを許可又は拒否すること

を特徴とするリモートアクセスプログラムが記録された記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、所定のリソースに対して遠隔地からアクセスするリモートアクセスシステム、リモートアクセス方法、リモートアクセスプログラム及びリモートアクセスプログラムが記録された記録媒体に関する。

【 0 0 0 2 】

【従来の技術】

近年、ネットワークに接続可能な情報家電等の各種機器が開発されており、これにともない、家庭内ネットワークをはじめとして様々な機器を対象としたネットワークが構築されつつある。また、このような状況に応じて、屋外等の遠隔地から屋内に設けられた各種情報家電又はパーソナルコンピュータ等の各種情報処理端末若しくはサーバ装置等に対して、ユーザが所持する携帯電話機や携帯情報端末機（Personal Digital Assistants；PDA）等の機器を用いてリモートアクセスすることによって享受できるサービスが各種提案されている。

【 0 0 0 3 】

このようなサービスにおいては、当該サービスを提供するサーバ装置等のハードウェアやソフトウェア、さらにはデータといった各種リソースに対する不正なユーザのアクセスを排除すべく、認証及びアクセス権の管理を行うことが必須とされている。

【 0 0 0 4 】

【発明が解決しようとする課題】

ところで、上述したサービスとしては、既に実施されているものもあり、個別に認証の仕組みを構築している。しかしながら、このようなサービスにおいては、個人単位の権限（操作）をも含めた認証方式が未だ確立されていないのが現状である。

【0 0 0 5】

また、個人単位の権限管理の手法としては、いわゆる I D (I D e n t i f i c a t i o n) パスワードを用いた認証方式があるが、この I D パスワードを用いた認証方式においては、仕組みが非常に煩雑となり、処理負担が大きいといった問題があった。

【0 0 0 6】

本発明は、このような実情に鑑みてなされたものであり、いわゆる属性証明書 (A t t r i b u t e C e r t i f i c a t e ; A C) を用いて権限管理を行うことにより、リモートアクセスを行う際に、リソースにアクセスする機器自体等のエンティティのみならず、アクセスさせたいリソース毎に、権限単位での制御を容易且つ安全に行うことができるリモートアクセスシステム、リモートアクセス方法、リモートアクセスプログラム及びリモートアクセスプログラムが記録された記録媒体を提供することを目的とする。

【0 0 0 7】

【課題を解決するための手段】

上述した目的を達成する本発明にかかるリモートアクセスシステムは、所定のリソースに対して遠隔地からアクセスするリモートアクセスシステムであって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器と、このアクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当する機器であるゲートウェイ機器と、少なくともリソースに対する権限が記述された電子証明書であり、且つ、この電子証明書を経由させるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持し、アクセス対象機器に対してアクセスするアクセス機器とを備え、アクセス機器は

、権限及び経由情報記述属性証明書をゲートウェイ機器に対して送信して提示し、ゲートウェイ機器は、アクセス機器から受信した権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定されたアクセス対象機器に対して送信して提示し、アクセス対象機器は、ゲートウェイ機器から受信した権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否することを特徴としている。

【 0 0 0 8 】

このような本発明にかかるリモートアクセスシステムは、少なくともリソースに対する権限とゲートウェイ機器の情報とを、権限及び経由情報記述属性証明書に記述し、この権限及び経由情報記述属性証明書を、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示し、リソースに対するアクセス機器のアクセスを検証する。

【 0 0 0 9 】

また、上述した目的を達成する本発明にかかるリモートアクセス方法は、所定のリソースに対して遠隔地からアクセスするリモートアクセス方法であって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を經由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経由情報記述属性証明書を保持させ、アクセス機器によって権限及び経由情報記述属性証明書をゲートウェイ機器に対して送信して提示し、ゲートウェイ機器によってアクセス機器から受信した権限及び経由情報記述属性証明書の内容を検証し、当該権限及び経由情報記述属性証明書をアクセスの対象として指定されたアクセス対象機器に対して送信して提示し、アクセス対象機器によってゲートウェイ機器から受信した権限及び経由情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否することを特徴としている。

【 0 0 1 0 】

このような本発明にかかるリモートアクセス方法は、少なくともリソースに対する権限とゲートウェイ機器の情報とを、権限及び経路情報記述属性証明書に記述し、この権限及び経路情報記述属性証明書を、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示し、リソースに対するアクセス機器のアクセスを検証する。

【 0 0 1 1 】

さらに、上述した目的を達成する本発明にかかるリモートアクセスプログラムは、所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なりモートアクセスプログラムであって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経路情報記述属性証明書が保持されており、アクセス機器からゲートウェイ機器を介して送信されて提示された権限及び経路情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否することを特徴としている。

【 0 0 1 2 】

このような本発明にかかるリモートアクセスプログラムは、少なくともリソースに対する権限とゲートウェイ機器の情報とが、権限及び経路情報記述属性証明書に記述されており、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示された権限及び経路情報記述属性証明書に基づいて、リソースに対するアクセス機器のアクセスを検証する。

【 0 0 1 3 】

さらにまた、上述した目的を達成する本発明にかかるリモートアクセスプログラムが記録された記録媒体は、所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なりモートアクセスプログラムが記録された記録媒体であ

って、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経路情報記述属性証明書が保持されており、リモートアクセスプログラムは、アクセス機器からゲートウェイ機器を介して送信されて提示された権限及び経路情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否することを特徴としている。

【 0 0 1 4 】

このような本発明にかかるリモートアクセスプログラムが記録された記録媒体は、少なくともリソースに対する権限とゲートウェイ機器の情報とが、権限及び経路情報記述属性証明書に記述されており、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示された権限及び経路情報記述属性証明書に基づいて、リソースに対するアクセス機器のアクセスを検証するリモートアクセスプログラムを提供する。

【 0 0 1 5 】

【発明の実施の形態】

以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

【 0 0 1 6 】

この実施の形態は、所定のリソースに対して遠隔地からアクセスするリモートアクセスシステムである。このリモートアクセスシステムは、ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission) 9594-8、又はITU-T X.509に基づく属性証明書 (Attribute Certificate; AC) を用いて権限管理を行うことにより、リモートアクセスを行う際に、リソースにアクセスする機器自体等のエンティティのみならず、アクセスさせたいリソース毎に、権限単位での制御を容易に

行うことができるものである。また、このリモートアクセスシステムは、属性証明書を利用する際に、リソースが属するネットワークの入り口となるゲートウェイを経由して、リソースとこのリソースにアクセスしようとする機器との間で属性証明書の授受を行うことにより、属性証明書の送付ルートを確認することを可能とし、セキュリティを向上させることができるものである。

【 0 0 1 7 】

まず、リモートアクセスシステムの説明に先だって、当該リモートアクセスシステムにて用いる電子証明書である公開鍵証明書 (Public Key Certificate ; P K C) 及び上述した属性証明書の概略について説明する。

【 0 0 1 8 】

まず、公開鍵証明書について説明する。公開鍵証明書は、いわゆる公開鍵暗号方式における独立した所定の第三者機関である証明書発行認証局 (Certification Authority ; C A 又は Issuer Authority ; I A) によって発行されるものである。

【 0 0 1 9 】

ここで、公開鍵暗号方式について説明する。公開鍵暗号方式は、発信者と受信者との鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵とし、他方の鍵を秘密に保つ秘密鍵とするものである。公開鍵暗号方式は、暗号化及び復号に共通の鍵を用いるいわゆる共通鍵暗号方式と異なり、秘密に保つ必要がある秘密鍵を特定の 1 人が持てばよいと、共通鍵暗号方式と比較して鍵の管理において有利である。公開鍵暗号方式の代表的なものとしては、いわゆる R S A (Rivest-Shamir-Adleman) 暗号がある。この R S A 暗号は、例えば 1 5 0 桁程度の非常に大きな 2 つの素数の積の素因数分解処理の困難性を利用するものである。

【 0 0 2 0 】

公開鍵暗号方式は、不特定多数のユーザに公開鍵を使用可能とするものであり、配布する公開鍵が正当なものであるか否かを証明するために公開鍵証明書を用いる方法が広く用いられている。例えば、公開鍵暗号方式においては、ある特定のユーザ A が対となる公開鍵と秘密鍵とを生成し、生成した公開鍵を証明書発行

認証局に対して送付して公開鍵証明書を取得し、この公開鍵証明書を一般に公開する。一方、不特定のユーザは、公開鍵証明書に基づいて所定の手続きを経ることによって公開鍵を取得し、平文たる文書等を暗号化して特定のユーザAに対して送付する。そして、ユーザAは、不特定のユーザから送付された暗号化文書を秘密鍵を用いて復号する等の処理を行う。公開鍵暗号方式は、このような暗号方式である。

【 0 0 2 1 】

また、公開鍵暗号方式においては、ユーザAは、秘密鍵を用いて平文たる文書等に署名を付加し、不特定のユーザが公開鍵証明書に基づいて所定の手続きを経ることによって公開鍵を取得し、その署名の検証を行うことが可能となる。例えば、公開鍵暗号方式においては、証明書発行認証局が公開鍵証明書を参照して公開鍵を判別すると、任意の平文たる文書等をユーザAに対して送付し、秘密鍵を用いて暗号化させ、再度送り返させる。証明書発行認証局は、ユーザAから送付された暗号化文書を公開鍵を用いて復号することにより、署名の正当性を検証することができる。

【 0 0 2 2 】

このような公開鍵暗号方式における公開鍵証明書は、管理者たるユーザが自己を識別するための情報や公開鍵等を証明書発行認証局に提出することにより、証明書発行認証局側が当該証明書発行認証局を識別するための情報や有効期限等の情報を付加し、さらに証明書発行認証局による署名を付加して作成される。

【 0 0 2 3 】

具体的には、公開鍵証明書は、図1及び図2に示すようなフォーマットから構成される。なお、同図においては、公開鍵証明書を構成する各フィールド毎の項目と、これらの各項目に対する説明とを記載している。

【 0 0 2 4 】

図1に示すバージョン (version) は、公開鍵証明書のフォーマットのバージョン情報を記述するフィールドであり、例えばフォーマットがバージョン3である場合にはバージョン3を示す“2”が記述される。

【 0 0 2 5 】

シリアルナンバ (serial Number) は、証明書発行認証局によって設定される公開鍵証明書のシリアルナンバを記述するフィールドであり、例えばシーケンシャルな番号が記述される。

【 0 0 2 6 】

署名アルゴリズム識別子、及びアルゴリズムパラメータ (signature algorithm Identifier algorithm parameters) は、公開鍵証明書の署名アルゴリズムを識別するための情報とそのパラメータとを記述するフィールドである。署名アルゴリズムとしては、例えば楕円曲線暗号又は R S A 暗号があり、署名アルゴリズムとして楕円曲線暗号が適用されている場合には、アルゴリズムパラメータとしてパラメータ及び鍵長が記述され、署名アルゴリズムとして R S A 暗号が適用されている場合には、アルゴリズムパラメータとして鍵長が記述される。

【 0 0 2 7 】

発行者 (issuer) は、公開鍵証明書の発行者、すなわち、証明書発行認証局の名称を識別可能とする形式 (Distinguished Name) で記述するフィールドである。

【 0 0 2 8 】

有効期限 (validity) は、公開鍵証明書の有効期限である開始日時 (not Before) 及び終了日時 (not After) を記述するフィールドである。

【 0 0 2 9 】

サブジェクト (subject) は、ユーザである認証対象者の名前を記述するフィールドであり、例えばユーザ機器の識別子やサービス提供主体の識別子等が記述される。

【 0 0 3 0 】

サブジェクト公開鍵情報 (subject Public Key Info algorithm subject Public key) は、ユーザの公開鍵情報としての鍵アルゴリズムや鍵情報自体を記述するフィールドであり、鍵アルゴリズムとしては、例えば楕円曲線暗号又は R S A 暗号がある。

【 0 0 3 1 】

これらの各フィールドは、公開鍵証明書のフォーマットがバージョン 1 以降の

バージョンであるものに含まれるフィールドであり、以下に示す各フィールドは、バージョン 3 であるものに追加されるフィールドである。

【 0 0 3 2 】

証明局鍵識別子 (authority Key Identifier-key Identifier, authority Certificate Issuer, authority Certificate Serial Number) は、証明書発行認証局の署名確認用の鍵を識別するための情報であり、8 進数表記の鍵識別番号、一般名称 (General Name) 形式の証明書発行認証局の名称、及び認証番号を記述するフィールドである。

【 0 0 3 3 】

サブジェクト鍵識別子 (subject key Identifier) は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を記述するフィールドである。

【 0 0 3 4 】

鍵使用目的 (key usage) は、鍵の使用目的を指定するフィールドであり、(0) デジタル署名用 (digital Signature)、(1) 否認防止用 (non Repudiation)、(2) 鍵の暗号化用 (key Encipherment)、(3) メッセージの暗号化用 (data Encipherment)、(4) 共通鍵配送用 (key Agreement)、(5) 認証の署名確認用 (key Certificate Sign)、(6) 失効リストの署名確認用 (CRL Sign)、(7) 鍵交換時 (key Agreement) データの暗号化にのみ利用 (encipher Only)、及び (8) 鍵交換時データの復号にのみ利用 (decipher Only) の各使用目的が設定される。

【 0 0 3 5 】

秘密鍵有効期限 (private Key Usage Period) は、ユーザが有する秘密鍵の有効期限である開始日時 (not Before) 及び終了日時 (not After) を記述するフィールドであり、デフォルトでは、公開鍵証明書の有効期限と公開鍵の有効期限と秘密鍵の有効期限とは互いに同一とされる。

【 0 0 3 6 】

図 2 に示す認証局ポリシー (Certificate Policy) は、証明書発行認証局の証明書発行ポリシーを記述するフィールドであり、例えば ISO/IEC 983

4-1 に準拠したポリシー ID (policy Identifier) や認証基準 (policy Qualifiers) が記述される。

【0037】

ポリシー・マッピング (policy Mappings) は、証明書発行認証局を認証する場合にのみ記述されるフィールドであり、証明書発行を行う証明書発行認証局のポリシー (issuer Domain Policy) と被認証ポリシー (subject Domain Policy) とのマッピングを規定する。

【0038】

サポート・アルゴリズム (supported Algorithms) は、ディレクトリ (X. 500) のアトリビュートを定義するフィールドである。サポート・アルゴリズムは、コミュニケーションの相手がディレクトリ情報を利用する場合に、事前にそのアトリビュートを知らせるのに用いる。

【0039】

サブジェクト別名 (subject Alt Name) は、ユーザの別名を一般名称 (General Name) 形式で記述するフィールドである。

【0040】

発行者別名 (issuer Alt Name) は、証明書発行者の別名を記述するフィールドである。

【0041】

サブジェクト・ディレクトリ・アトリビュート (subject Directory Attributes) は、ユーザの任意の属性を記述するフィールドである。

【0042】

基本制約 (basic Constraints) は、証明対象の公開鍵が証明書発行認証局の署名用であるかユーザのものであるかを区別するためのフィールドである。

【0043】

許容サブツリー制約名 (name Constraints permitted Subtrees) は、被認証者が証明書発行認証局である場合にのみ使用される公開鍵証明書の有効領域を示すフィールドである。

【0044】

制約ポリシー (policy Constraints) は、認証パスの残りに対する明確な認証ポリシー ID や禁止ポリシーマップを要求する制限を記述するフィールドである。

【0045】

CRL 参照ポイント (Certificate Revocation List Distribution Points) は、ユーザが公開鍵証明書を利用する際に、この公開鍵証明書が失効していないかどうかを確認するための失効リストの参照ポイントを記述するフィールドである。

【0046】

署名は、公開鍵証明書発行者、すなわち、証明書発行認証局の署名フィールドである。電子署名は、公開鍵証明書の全体に対していわゆるハッシュ関数を適用してハッシュ値を生成し、このハッシュ値に対して証明書発行認証局の秘密鍵を用いて暗号化して生成したデータである。

【0047】

証明書発行認証局は、このようなフォーマットからなる公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行ったユーザの排斥を行うための不正者リストの作成、管理、配布、すなわち、リボケーション (revocation) を行う。また、証明書発行認証局は、必要に応じて、公開鍵及び秘密鍵の生成も行う。

【0048】

一方、この公開鍵証明書を利用するユーザは、自己が有する証明書発行認証局の公開鍵を用いて当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功すると、公開鍵証明書に基づいて公開鍵を取得し、この公開鍵を利用することができる。したがって、公開鍵証明書を利用する全てのユーザは、当該公開鍵証明書を発行した証明書発行認証局の公開鍵を有しているか取得する必要がある。

【0049】

リモートアクセスシステムにおいては、後述するように、このような公開鍵証明書を各エンティティに保持させる。

【0050】

つぎに、属性証明書について説明する。属性証明書は、証明書発行認証局とは異なるローカルな機関である属性認証局 (Attribute Authority; AA) によって発行されるものである。

【 0 0 5 1 】

属性証明書は、図 3 及び図 4 に示すようなフォーマットから構成される。なお、同図においては、属性証明書を構成する各フィールド毎の項目と、これらの各項目に対する説明とを記載している。

【 0 0 5 2 】

図 3 に示すバージョン (version) は、属性証明書のフォーマットのバージョン情報を記述するフィールドであり、例えばフォーマットがバージョン 2 (1) である場合にはバージョン 2 (1) を示す "1" が記述される。

【 0 0 5 3 】

ホルダー (holder) は、属性証明書が結び付けられた公開鍵証明書の所有者を特定するためのフィールドである。ホルダーには、ベース認証局識別子 (base Certificate ID) として、属性証明書の所有者が有する公開鍵証明書の発行者名 (issuer)、属性証明書の所有者が有する公開鍵証明書のシリアルナンバ (serial)、属性証明書の所有者が有する公開鍵証明書の発行者を識別するための固有の識別子 (issuer UID) が記述される。また、ホルダーには、公開鍵証明書におけるサブジェクト (subject) 又はサブジェクト別名 (subject Alt Name) と同一とされる属性証明書の所有者の名称 (entity name) が記述される。さらに、ホルダーには、将来、属性証明書が識別情報 (identity) や公開鍵証明書にリンクされていない場合を想定して、例えば公開鍵のハッシュが記述されるオブジェクト・ダイジェスト情報 (object Digest Info) が記述される。

【 0 0 5 4 】

発行者 (issuer) は、属性証明書に署名した発行者の情報を指定するフィールドである。

【 0 0 5 5 】

署名 (signature) は、属性証明書の署名を有効にするために使用するアルゴリズムを識別するための識別子を記述するフィールドである。

【 0 0 5 6 】

シリアルナンバ (serial Number) は、属性認証局が各属性証明書に割り振るシリアルナンバを記述するフィールドである。

【 0 0 5 7 】

属性証明書有効期限 (attr Cert Validity Period) は、属性証明書の有効期限である開始日時 (not Before) 及び終了日時 (not After) を記述するフィールドである。

【 0 0 5 8 】

図 4 に示す属性 (attributes) は、属性証明書の所有者の特権に関する情報を記述するフィールドであり、例えば、文章でアクセスが許可された対象物を記述してもよく、システム側で用意しておいたアクセスすることができるコードを記述してもよく、ある平文を暗号化する鍵を記述してもよい。例えば、属性には、属性証明書の検証者が当該属性証明書の所有者を認証する場合に利用するサービスに関する認証情報 (Service Authentication Information)、属性証明書の検証者が用いる当該属性証明書の所有者のアクセス許可情報 (Access Identity)、課金のために属性証明書の所有者を特定するための情報 (Charging Identity)、属性証明書の所有者のグループへの帰属関係を示す情報 (Group)、属性証明書の所有者に与えられる役割を示す情報 (Role)、属性証明書の所有者に対する秘密情報の使用許可に関する情報 (Clearance) が記述される。

【 0 0 5 9 】

発行者固有識別子 (issuer Unique ID) は、属性証明書の発行者の公開鍵証明書で指定されている場合に利用されるフィールドである。

【 0 0 6 0 】

拡張情報 (extensions) は、属性証明書の所有者の情報ではなく属性証明書の情報を記述するフィールドであり、サーバ及び／又はサービス管理者が属性証明書の所有者の監査を行い不正行為の検出、すなわち特定をするために用いる情報 (Audit Identity)、属性証明書が対象とするサーバ及び／又はサービスを示す情報 (AC Targeting)、属性証明書の検証者による当該属性証明書の署名確認の補助情報である属性証明書の発行者の鍵情報 (Authority Key)、属性証明書の

検証者による当該属性証明書失効状態確認の補助情報である O C S P レスポ
 ンダの U R I (Uniform Resource Identifiers) を示す情報 (Authority Informat
 ion Access)、属性証明書の検証者による当該属性証明書失効状態確認の補助
 情報である C R L (Certificate Revocation List) 配布点の U R I を示す情報
 (CRL Distribution)、当該属性証明書に対応する失効情報がないことを示す情
 報 (No Revocation)、提出者が所有者以外である場合に利用され、属性証明書
 を提出することができるエンティティを示す情報 (Proxy Info) が記述される。

【 0 0 6 1 】

署名 (signature Value) は、属性認証局によってつけられた署名を記述する
 フィールドである。

【 0 0 6 2 】

リモートアクセスシステムにおいては、後述するように、このようなフォーマ
 ットからなる属性証明書を各エンティティに保持させることにより、あるエンテ
 イティに対していかなる権限が許可されているのかを検証することができる。

【 0 0 6 3 】

リモートアクセスシステムは、以上のような公開鍵証明書及び属性証明書を
 用いて構築される。

【 0 0 6 4 】

以下、これらの公開鍵証明書及び属性証明書を用了リモートアクセスシス
 テムについて説明する。

【 0 0 6 5 】

まず、リモートアクセスシステムの概念について説明する。なお、ここでは、
 説明の便宜上、家庭内に設けられた各種情報家電又はパーソナルコンピュータ等
 の各種情報処理端末若しくはサーバ装置等をアクセスの対象とし、これらの機器
 に対して携帯電話機や携帯情報端末機 (Personal Digital Assistants ; P D A
) 等の携帯機器を所持するユーザが屋外からアクセスするものとして説明する。

【 0 0 6 6 】

リモートアクセスシステムは、I T U - T (International Telecommunicatio
 n Union-Telecommunication sector) X. 5 0 9 で定義されている P M I (Pr

ivilege management Infrastructure) の機能の 1 つである属性証明書を用いた権限プロキシ機能により、アクセスさせたいリソース毎に、権限単位での制御を行う。

【 0 0 6 7 】

ここで、権限プロキシ機能について図 5 を用いて説明する。

【 0 0 6 8 】

同図に示すように、属性証明書 AC を保持するクライアント CL と、このクライアント CL の権限を検証する権限検証側サーバ VR との間に、クライアント CL の権限を主張する権限主張側サーバ AS が介在するシステムを考える。

【 0 0 6 9 】

この場合、クライアント CL は、権限検証側サーバ VR に対してアクセスしようとする際には、権限主張側サーバ AS に対して属性証明書 AC を提示し、これに応じて、権限主張側サーバ AS は、クライアント CL から提示された属性証明書 AC を、権限検証側サーバ VR に対して提示する。

【 0 0 7 0 】

しかしながら、この場合、権限検証側サーバ VR は、権限主張側サーバ AS から提示された属性証明書 AC が、権限主張側サーバ AS の属性証明書ではないことから、アクセスを許可しない旨の検証結果を出すことになる。すなわち、このようなシステムにおいては、属性証明書を直接的に授受する装置間で、権限の主張及び検証が行われることから、クライアント CL が権限検証側サーバ VR に対して自己の権限を主張しようとする際には、クライアント CL から権限検証側サーバ VR に対して直接的に属性証明書 AC を提示する必要がある。

【 0 0 7 1 】

そこで、このようなシステムにおいては、先に図 4 に示した拡張情報 (extensions) におけるプロキシ情報 (Proxy Info) を利用する。このプロキシ情報は、上述したように、属性証明書の提出者が所有者以外である場合に利用され、属性証明書を提出することができるエンティティを示す情報である。

【 0 0 7 2 】

したがって、このようなシステムにおいては、クライアント CL は、権限検証

側サーバVRに対してアクセスしようとする際には、属性証明書を提出できるエンティティとして権限検証側サーバVRを含む旨を示すプロキシ情報を記述した属性証明書ACを権限主張側サーバASに対して提示し、これに応じて、権限主張側サーバASは、クライアントCLから提示された属性証明書ACを、権限検証側サーバVRに対して提示する。

【 0 0 7 3 】

これにより、権限検証側サーバVRは、権限主張側サーバASから提示された属性証明書ACにおけるプロキシ情報を参照して当該属性証明書ACを検証し、アクセスを許可する旨の検証結果を出すことが可能となる。

【 0 0 7 4 】

このように、属性証明書ACを保持するクライアントCLと、このクライアントCLの権限を検証する権限検証側サーバVRとの間に、クライアントCLの権限を主張する権限主張側サーバASが介在するシステムにおいては、プロキシ情報に属性証明書ACの提出先を記述することにより、クライアントCLが権限検証側サーバVRに対してアクセスすることが可能となる。

【 0 0 7 5 】

リモートアクセスシステムは、このような権限プロキシ機能を利用する。概念的には、リモートアクセスシステムは、図6に示すように、上述した公開鍵証明書を発行する証明書発行認証局CAと、上述した属性証明書を発行する属性認証局AAと、アクセスの対象となる対象機器10₁、10₂と、これらの対象機器10₁、10₂が属する家庭内ネットワークと他のネットワークとを相互に接続するためのインターフェースであるホームゲートウェイと20と、対象機器10₁、10₂に対してアクセスするためにユーザが所持する携帯機器30とを、エンティティとして備える。

【 0 0 7 6 】

証明書発行認証局CAは、公開鍵暗号方式における独立した所定の第三者機関であって、ISO/IEC 9594-8、又はITU-T X.509に基づく電子証明書である公開鍵証明書を発行する。具体的には、証明書発行認証局CAは、公開鍵証明書PKC_{T1}、PKC_{T2}を、それぞれ、対象機器10₁、1

0₂に対して発行するとともに、公開鍵証明書PKC_Gをホームゲートウェイ20に対して発行するとともに、公開鍵証明書PKC_Mを携帯機器30に対して発行する。なお、この公開鍵証明書の発行の形態は、様々なものが考えられるが、例えば、対象機器10₁、10₂、ホームゲートウェイ20、及び携帯機器30の製造時にデータとして埋め込むことが考えられる。

【0077】

属性認証局AAは、証明書発行認証局CAとは論理的に異なるローカルな機関であって、権限管理を行うために用いる電子証明書である属性証明書を発行する。属性認証局AAは、証明書発行認証局CAからホームゲートウェイ20に対して発行された公開鍵証明書PKC_Gにより、ホームゲートウェイ20の認証を行う。そして、属性認証局AAは、例えばホームゲートウェイ20がユーザサイドに渡ってから初回接続時等に、携帯機器30に対して属性証明書AC_Pを発行する許可を与えるための属性証明書AC_Lを、ホームゲートウェイ20に対して発行する。なお、この属性証明書AC_Lについては、後に詳述するものとする。

【0078】

対象機器10₁、10₂は、それぞれ、図5における権限検証側サーバVRに相当するものである。対象機器10₁、10₂は、それぞれ、例えば、ネットワークに接続可能な各種情報家電や、パーソナルコンピュータ等の各種情報処理端末若しくはホームサーバ等のサーバ装置を想定したものであり、家庭内ネットワークを構成する機器である。なお、本発明におけるリソースとは、後に具体的な適用例を述べるように、ログインするこれらの対象機器10₁、10₂そのものを示す場合がある他、これらの対象機器10₁、10₂が保持するファイル等のデータやその他の各種情報を含む概念であるが、ここでは説明の便宜上、対象機器10₁、10₂そのものをリソースとするものとして説明する。対象機器10₁、10₂は、それぞれ、証明書発行認証局CAによって発行された公開鍵証明書PKC_{T1}、PKC_{T2}を保持し、これらの公開鍵証明書PKC_{T1}、PKC_{T2}を用いてホームゲートウェイ20との間で相互認証を行う。また、対象機器10₁、10₂は、それぞれ、携帯機器30がアクセスする際に送信した属性証明書AC_Pをホームゲートウェイ20を介して受信し、この属性証明書AC_Pの

検証を行う。

【 0 0 7 9 】

ホームゲートウェイ 2 0 は、図 5 における権限主張側サーバ A S に相当するものである。ホームゲートウェイ 2 0 は、例えば、いわゆるホームルータ、ファイアウォール、及び／又はブリッジといった概念を含むものであり、異なるプロトコルのネットワーク同士の接続を可能とするネットワークの入り口に相当する機器であり、対象機器 1 0₁、1 0₂ が属する家庭内ネットワークと他のネットワークとを相互に接続するためのインターフェースとして機能する。ホームゲートウェイ 2 0 は、証明書発行認証局 C A によって発行された公開鍵証明書 P K C_G を保持し、この公開鍵証明書 P K C_G を用いて対象機器 1 0₁、1 0₂、携帯機器 3 0、及び属性認証局 A A との間で相互認証を行う。また、ホームゲートウェイ 2 0 は、携帯機器 3 0 に対して属性証明書 A C_P を発行する許可を与えるための属性証明書 A C_L が属性認証局 A A によって発行されると、この属性証明書 A C_L を保持し、この属性証明書 A C_L に基づいて、携帯機器 3 0 に対して属性証明書 A C_P を発行する。なお、この属性証明書 A C_P については、後に詳述するものとする。さらに、ホームゲートウェイ 2 0 は、携帯機器 3 0 から送信された属性証明書 A C_P を受信すると、この属性証明書 A C_P を対象機器 1 0₁、1 0₂ のそれぞれに対して送信して提示する。

【 0 0 8 0 】

携帯機器 3 0 は、図 5 におけるクライアント C L に相当するものである。携帯機器 3 0 は、屋外にいるユーザが所持する携帯電話機や携帯情報端末機等の機器であり、いわゆるインターネット等のセキュアでないネットワーク N T を介してホームゲートウェイ 2 0 に対して接続可能とされる。携帯機器 3 0 は、証明書発行認証局 C A によって発行された公開鍵証明書 P K C_M を保持し、この公開鍵証明書 P K C_M を用いてホームゲートウェイ 2 0 との間で相互認証を行う。また、携帯機器 3 0 は、リソースとしての対象機器 1 0₁、1 0₂ のそれぞれに対してアクセスすることを認証するための属性証明書 A C_P がホームゲートウェイ 2 0 によって発行されると、この属性証明書 A C_P を I C (Integrated Circuit) カード等に格納すること等によって保持する。そして、携帯機器 3 0 は、対象機器

10_1 , 10_2 のそれぞれに対してアクセスしようと試みる際に、ICカード等に格納された属性証明書 AC_P を用いたログイン操作を行うことにより、この属性証明書 AC_P をホームゲートウェイ 20 に対して送信して提示する。

【0081】

このようなりモートアクセスシステムにおいては、上述したように、2つの属性証明書 AC_L , AC_P が使用される。

【0082】

まず、属性証明書 AC_L について説明する。

【0083】

属性証明書 AC_L は、上述したように、携帯機器 30 に対して属性証明書 AC_P を発行する許可をホームゲートウェイ 20 に対して与えるために、属性認証局 AA からホームゲートウェイ 20 に対して発行されるものである。例えば、この属性証明書 AC_L には、図 7 にタイプとして登録されているオブジェクト ID (Object ID; OI D) 及び値の例の抜粋を示す先に図 4 に示した属性 (attribute s) における各フィールドのうち、当該属性証明書 AC_L の所有者たるホームゲートウェイ 20 に与えられる役割を示す情報 (Role) を用いて、携帯機器 30 に対して属性証明書 AC_P を発行する許可を与える旨を示す情報を記述することができる。

【0084】

ここで、“ロール (Role)” の概念について説明する。

【0085】

この“ロール (Role)” の概念を用いた権限管理の手法は、本件出願人が先に出願している特願 2002-029636 に記載したものである。

【0086】

すなわち、この権限管理の手法においては、概念的には、図 8 に示すように、例えば権限 AU_{11} , AU_{12} , \dots , AU_{21} , AU_{22} , \dots といった所定の権限を定義する枠組みを 1 つの役割 (ロール) R_1 , R_2 とし、例えば個人 M_1 , M_2 , M_3 といった少なくとも 1 人以上の個人がこのロール R_1 , R_2 に属するものとされる。

【 0 0 8 7 】

この権限管理の手法においては、各個人 M_1 、 M_2 、 M_3 がそれぞれ有する属性証明書であって当該個人 M_1 、 M_2 、 M_3 が属しているロールを示す情報が記述されている役割割当証明書 (Role Assignment Certificate) R A A C が、属性認証局 A A によって発行されるとともに、ロール毎に発行される属性証明書であって当該ロールに許可されている権限を示す情報が記述されている役割定義証明書 (Role Specification Certificate) R S A C が、役割認証局 (Role Authority) R A によって発行される。なお、役割認証局 R A は、属性認証局 A A と同一であってもよいが、ここでは説明の便宜上、論理的に独立な機関であるものとする。

【 0 0 8 8 】

この権限管理の手法においては、各ロールの定義については、役割認証局 R A によって発行される役割定義証明書 R S A C を用いる。すなわち、この権限管理の手法においては、ロール毎に、許可される手続きが定義されるが、この情報が、役割認証局 R A によって発行される役割定義証明書 R S A C に記述される。

【 0 0 8 9 】

この役割定義証明書 R S A C は、先に図 3 及び図 4 に示した属性証明書のフォーマットにしたがって作成されるものであり、少なくとも、当該役割定義証明書 R S A C の発行者たる役割認証局 R A の名前を示す情報、ロールを識別するためのロール名といったロールの情報、システムによってコード又は操作名が記述されるものであって許可される操作を示す情報等の各種情報が記述される。

【 0 0 9 0 】

リモートアクセスシステムにおいては、携帯機器 3 0 に対して属性証明書 A C_Pを発行する許可を与える旨を示す情報を含む各種情報が記述された役割定義証明書 R S A C が役割認証局 R A によって発行され、権限 A U_{1 1}、A U_{1 2}、
 ・ ・ ・、A U_{2 1}、A U_{2 2}、
 ・ ・ ・ が定義されたリソース、すなわち、先に示した図 6 においては対象機器 1 0₁、1 0₂がこの役割定義証明書 R S A C を保持する。

【 0 0 9 1 】

一方、この権限管理の手法においては、各ロールに対する役割の割り当てについては、属性認証局 A A によって発行される役割割当証明書 R A A C を用いる。すなわち、この権限管理の手法においては、個人 M_1 , M_2 , M_3 毎に、各役割が定義されるが、この情報が、属性認証局 A A によって発行される役割割当証明書 R A A C に記述される。

【 0 0 9 2 】

この役割割当証明書 R A A C も、役割定義証明書 R S A C と同様に、先に図 3 及び図 4 に示した属性証明書のフォーマットにしたがって作成されるものであり、少なくとも、当該役割割当証明書 R A A C の発行者たる属性認証局 A A の名前を示す情報、ロールを識別するためのロール名といったロールの情報、対応する役割定義証明書 R S A C と関連付けを行うための役割定義証明書 R S A C への参照ポイントを示す情報としての役割認証局 R A の名前を示す情報等の各種情報が記述される。

【 0 0 9 3 】

リモートアクセスシステムにおいては、このような各種情報が記述された役割割当証明書 R A A C が属性証明書 A C _L として属性認証局 A A によって発行され、個人 M_1 , M_2 , M_3 、すなわち、先に示した図 6 においてはホームゲートウェイ 2 0 が、この役割割当証明書 R A A C を保持する。

【 0 0 9 4 】

リモートアクセスシステムにおいては、このような“ロール (Role)”の概念を用いることにより、携帯機器 3 0 に対して属性証明書 A C _P を発行する許可を与える旨を示す情報を記述した属性証明書 A C _L を、属性認証局 A A によってホームゲートウェイ 2 0 に対して発行することができる。これにより、リモートアクセスシステムにおいては、この属性証明書 A C _L を保持したホームゲートウェイ 2 0 によって属性証明書 A C _P を携帯機器 3 0 に対して発行することが可能となる。

【 0 0 9 5 】

なお、リモートアクセスシステムにおいては、携帯機器 3 0 に対して属性証明書 A C _P を発行する許可を与える旨を示す情報を属性証明書 A C _L に記述するた

めに、当該属性証明書 AC_L の所有者たるホームゲートウェイ 20 に与えられる役割を示す情報 (Role) を用いるのではなく、図 7 に示した属性 (attributes) における各フィールドのうち、属性証明書の検証者が当該属性証明書の所有者を認証する場合に利用するサービスに関する認証情報 (Service Authentication Information) や、属性証明書の検証者が用いる当該属性証明書の所有者のアクセス許可情報 (Access Identity) 等を用いて、同情報を記述することも可能である。

【 0 0 9 6 】

また、リモートアクセスシステムにおいては、権限委譲エクステンションを用い、属性証明書 AC_P を発行する対象及び権限を制御するようにしてもよい。例えば、リモートアクセスシステムにおいては、Basic Attribute Constraints エクステンションを用いて、ホームゲートウェイ 20 には携帯機器 30 に対して属性証明書 AC_P を発行できる旨を示し、さらに、ホームゲートウェイ 20 からは権限委譲を許可しない旨を設定することが考えられる。

【 0 0 9 7 】

このように、リモートアクセスシステムにおいては、携帯機器 30 に対して属性証明書 AC_P を発行する許可をホームゲートウェイ 20 に与える手法として、様々なものが考えられる。

【 0 0 9 8 】

つぎに、属性証明書 AC_P について説明する。

【 0 0 9 9 】

属性証明書 AC_P は、ある公開鍵証明書を保持している機器又はユーザに対する権限が記述されたものであり、ここでは、公開鍵証明書 PKC_M を保持している携帯機器 30 に対する権限として、リソースとしての対象機器 10_1 、 10_2 のそれぞれに対してアクセスすることを許可する旨の情報が記述されたものである。例えば、この属性証明書 AC_P には、先に図 7 に示した属性 (attributes) における各フィールドのうち、属性証明書 AC_P の検証者たる対象機器 10_1 、 10_2 のそれぞれが当該属性証明書 AC_P の所有者を認証する場合に利用するサービスに関する認証情報 (Service Authentication Information) や、属性証明

書 AC_P の検証者たる対象機器 10_1 , 10_2 のそれぞれが用いる当該属性証明書 AC_P の所有者のアクセス許可情報 (Access Identity) 等を用いて、アクセスする対象、アクセスできる操作 (権限)、及びアクセスするための認証情報がある場合には当該認証情報を記述することができる。また、属性証明書 AC_P には、図 9 にタイプとして登録されているオブジェクト ID (Object ID; OID) 及びクリティカル又は値の例の抜粋を示す先に図 4 に示した拡張情報 (extensions) における各フィールドのうち、プロキシ情報 (Proxy Info) を用いて、当該属性証明書 AC_P を経由させるホームゲートウェイ 20 の情報が記述される。

【0100】

ここで、プロキシ情報は、具体的には、図 10 に示すように記述されるものである。

【0101】

属性証明書 AC_P には、このようなプロキシ情報におけるターゲット (Target) として、ホームゲートウェイ 20 を識別するためのアドレスや識別子が記述されるとともに、ホームゲートウェイ 20 が保持する公開鍵証明書 PKC_G を示す情報が記述される。

【0102】

このように、リモートアクセスシステムにおいては、携帯機器 30 に対する権限として、リソースとしての対象機器 10_1 , 10_2 のそれぞれに対してアクセスすることを許可する旨の情報が記述されるとともに、プロキシ情報として、ホームゲートウェイ 20 の情報が記述された属性証明書 AC_P を、ホームゲートウェイ 20 から携帯機器 30 に対して発行することができる。これにより、リモートアクセスシステムにおいては、対象機器 10_1 , 10_2 が、それぞれ、この属性証明書 AC_P をホームゲートウェイ 20 を介して受信した場合には、プロキシ情報におけるターゲットを検証し、且つ、ホームゲートウェイ 20 から送信された属性証明書であることを検証することになる。

【0103】

さて、このようなりモートアクセスシステムにおいては、具体的には、図 11 に示すように、当該リモートアクセスシステムを構築するための準備フェーズ P

1 が行われると、任意の携帯機器をリソースに対してアクセスする機器として登録するための登録フェーズ P 2 が行われる。これにより、リモートアクセスシステムにおいては、登録された携帯機器が任意の操作を行うことが可能となり、実際に携帯機器が任意の操作を行う際には、アクセスフェーズ P 3 が行われる。また、リモートアクセスシステムにおいては、必要に応じて、任意の携帯機器をリソースに対してアクセスする機器から除外するためのアクセス削除フェーズ P 4 や、任意の携帯機器の権限を変更するためのアクセス変更フェーズ P 5 が行われる。

【 0 1 0 4 】

以下、これら 5 つの各フェーズについて説明する。

【 0 1 0 5 】

まず、準備フェーズ P 1 について説明する。

【 0 1 0 6 】

リモートアクセスシステムにおいては、当該リモートアクセスシステムを構築するための準備フェーズ P 1 として、各エンティティが相互認証可能となるように、証明書発行認証局 C A により、各エンティティに対して認証のための公開鍵証明書を発行する。すなわち、リモートアクセスシステムにおいては、上述したように、各エンティティの製造時等に、証明書発行認証局 C A により、公開鍵証明書 PKC_{T1} 、 PKC_{T2} を、それぞれ、対象機器 10_1 、 10_2 に対して発行するとともに、公開鍵証明書 PKC_G をホームゲートウェイ 20 に対して発行するとともに、公開鍵証明書 PKC_M を携帯機器 30 に対して発行する。

【 0 1 0 7 】

リモートアクセスシステムは、このような準備フェーズ P 1 を経ることにより、各エンティティが相互認証可能な状態に構築される。

【 0 1 0 8 】

つぎに、登録フェーズ P 2 について説明する。

【 0 1 0 9 】

リモートアクセスシステムにおいては、任意の携帯機器としての携帯機器 30 をリソースに対してアクセスする機器として登録するための登録フェーズ P 2 と

して、図 1 2 に示す工程が行われる。

【0 1 1 0】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップ S 1 において、属性認証局 A A により、上述した準備フェーズ P 1 にて証明書発行認証局 C A によって発行されてホームゲートウェイ 2 0 に保持されている公開鍵証明書 P K C_G を用いて、ホームゲートウェイ 2 0 との間で相互認証を行う。この相互認証は、ホームゲートウェイ 2 0 自体に対する認証であり、ホームゲートウェイ 2 0 が正当なものであるか否かを認証するためのものである。

【0 1 1 1】

続いて、リモートアクセスシステムにおいては、ステップ S 2 において、属性認証局 A A により、ホームゲートウェイ 2 0 がユーザサイドに渡ってから初回接続時等に、携帯機器 3 0 に対して属性証明書 A C_P を発行する許可を与えるための属性証明書 A C_L を、ホームゲートウェイ 2 0 に対して発行する。これにともない、ホームゲートウェイ 2 0 は、属性認証局 A A から送信された属性証明書 A C_L を保持する。

【0 1 1 2】

続いて、リモートアクセスシステムにおいては、ステップ S 3 において、ホームゲートウェイ 2 0 により、ユーザからの指示にしたがい、接続する機器、すなわち、対象機器 1 0₁、1 0₂ のそれぞれの情報を登録するとともに、その対象機器 1 0₁、1 0₂ のそれぞれに対してリモートからアクセスしてもよい携帯機器 3 0 に対して上述したプロシキ情報を記述した属性証明書 A C_P を発行する。

【0 1 1 3】

続いて、リモートアクセスシステムにおいては、ステップ S 4 において、携帯機器 3 0 により、上述した準備フェーズ P 1 にて証明書発行認証局 C A によって発行されて保持している公開鍵証明書 P K C_M を用いて、ホームゲートウェイ 2 0 との間で相互認証を行う。

【0 1 1 4】

そして、リモートアクセスシステムにおいては、ステップ S 5 において、携帯機器 3 0 により、ホームゲートウェイ 2 0 から送信された属性証明書 A C_P を I

Cカード等に格納して保持し、一連の登録フェーズP 2を終了する。

【0 1 1 5】

リモートアクセスシステムにおいては、このような一連の工程からなる登録フェーズP 2を経ることにより、リソースに対してアクセスする機器として、携帯機器3 0を登録することができる。このようにしてリソースに対してアクセスする携帯機器3 0の登録がされたリモートアクセスシステムにおいては、登録された携帯機器3 0が任意の操作を行うことが可能となる。

【0 1 1 6】

つぎに、アクセスフェーズP 3について説明する。

【0 1 1 7】

リモートアクセスシステムにおいては、登録された携帯機器3 0がリソースに対してアクセスする際には、アクセスフェーズP 3として、図1 3に示す工程が行われる。

【0 1 1 8】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップS 1 1において、携帯機器3 0により、保持している公開鍵証明書 PKC_M を用いて、ホームゲートウェイ2 0との間で相互認証を行う。

【0 1 1 9】

続いて、リモートアクセスシステムにおいては、ステップS 1 2において、携帯機器3 0により、保持している属性証明書 AC_P をホームゲートウェイ2 0に対して送信して提示する。

【0 1 2 0】

これに応じて、リモートアクセスシステムにおいては、ステップS 1 3において、ホームゲートウェイ2 0により、携帯機器3 0から提示された属性証明書 AC_P の内容に基づいて、当該属性証明書 AC_P を、アクセスする対象として指定された機器、すなわち、対象機器 10_1 、 10_2 のいずれか又は双方に対して送信して提示する。

【0 1 2 1】

続いて、リモートアクセスシステムにおいては、ステップS 1 4において、対

対象機器 10_1 , 10_2 のいずれか又は双方により、ホームゲートウェイ 20 から送信された属性証明書 AC_P を受信し、上述したプロシキ情報や属性といった当該属性証明書 AC_P の内容を検証する。

【0122】

リモートアクセスシステムにおいては、ステップ S15 において、属性証明書 AC_P の検証結果が正当なものであった場合には、ステップ S16 において、対象機器 10_1 , 10_2 のいずれか又は双方によって携帯機器 30 のアクセスを許可し、一連のアクセスフェーズ P3 を終了する。一方、リモートアクセスシステムにおいては、ステップ S15 において、属性証明書 AC_P の検証結果が不当なものであった場合には、ステップ S17 において、対象機器 10_1 , 10_2 のいずれか又は双方によって携帯機器 30 のアクセスを拒否し、一連のアクセスフェーズ P3 を終了する。

【0123】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセスフェーズ P3 を経ることにより、対象機器 10_1 , 10_2 のそれぞれによって携帯機器 30 の権限を判別することができ、アクセスが許可された携帯機器 30 は、任意の操作を行うことが可能となる。

【0124】

つぎに、アクセス削除フェーズ P4 について説明する。

【0125】

リモートアクセスシステムにおいては、任意の携帯機器をリソースに対してアクセスする機器から除外したい場合には、アクセス削除フェーズ P4 として、図 14 に示す工程が行われる。

【0126】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップ S21 において、ホームゲートウェイ 20 により、ユーザからの指示にしたがい、対象機器 10_1 , 10_2 のそれぞれに対してリモートからアクセスしてもよい携帯機器 30 に対して発行した属性証明書 AC_P に対する CRL (ACRL) を作成し、この CRL (ACRL) を保持する。

【 0 1 2 7 】

このように、リモートアクセスシステムにおいては、属性証明書 AC_P に対する $CRL (ACRL)$ を作成することにより、携帯機器 30 からホームゲートウェイ 20 に対してアクセスがあった場合には、ホームゲートウェイ 20 によってアクセスを拒否することができ、携帯機器 30 をリソースに対してアクセスする機器から除外することができる。特に、リモートアクセスシステムは、複数人のユーザの間で携帯機器 30 の貸借がある場合や携帯機器 30 を紛失した場合といった携帯機器 30 の側の都合による場合等には、属性証明書 AC_P に対する $CRL (ACRL)$ を作成するのみで、携帯機器 30 をリソースに対してアクセスする機器から除外することができる。

【 0 1 2 8 】

ただし、リモートアクセスシステムにおいては、このような操作を繰り返し行うことにより、 $CRL (ACRL)$ のサイズが大きくなり、取り扱いに不便を生じるおそれがある。

【 0 1 2 9 】

そこで、リモートアクセスシステムにおいては、正当なユーザが自らの意思で携帯機器 30 をリソースに対してアクセスする機器から除外したい場合等には、ステップ S 2 1 の処理に続いて、以下のステップ S 2 2 乃至ステップ S 2 4 の処理を行うようにしてもよい。

【 0 1 3 0 】

すなわち、リモートアクセスシステムにおいては、ステップ S 2 2 において、携帯機器 30 により、保持している公開鍵証明書 PKC_M を用いて、ホームゲートウェイ 20 との間で相互認証を行う。

【 0 1 3 1 】

続いて、リモートアクセスシステムにおいては、ステップ S 2 3 において、ホームゲートウェイ 20 からの指示にしたがい、携帯機器 30 により、保持している属性証明書 AC_P を削除する。

【 0 1 3 2 】

そして、リモートアクセスシステムにおいては、ステップ S 2 4 において、ホ

ームゲートウェイ 2 0 により、ステップ S 2 1 にて作成した C R L (A C R L) を削除し、一連のアクセス削除フェーズ P 4 を終了する。

【 0 1 3 3 】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセス削除フェーズ P 4 を経ることにより、携帯機器 3 0 をリソースに対してアクセスする機器から除外することができる。

【 0 1 3 4 】

最後に、アクセス変更フェーズ P 5 について説明する。

【 0 1 3 5 】

リモートアクセスシステムにおいては、任意の携帯機器の権限を変更したい場合には、アクセス変更フェーズ P 5 として、図 1 5 に示す工程が行われる。

【 0 1 3 6 】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップ S 3 1 において、ホームゲートウェイ 2 0 により、ユーザからの指示にしたがい、携帯機器 3 0 に対してプロシキ情報を記述した新たな属性証明書 A C _P を発行する。

【 0 1 3 7 】

続いて、リモートアクセスシステムにおいては、ステップ S 3 2 において、携帯機器 3 0 により、保持している公開鍵証明書 P K C _M を用いて、ホームゲートウェイ 2 0 との間で相互認証を行う。

【 0 1 3 8 】

そして、リモートアクセスシステムにおいては、ステップ S 3 3 において、携帯機器 3 0 により、ホームゲートウェイ 2 0 から送信された新たな属性証明書 A C _P を、元の属性証明書 A C _P と置換して I C カード等に格納して保持し、一連のアクセス変更フェーズ P 5 を終了する。

【 0 1 3 9 】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセス変更フェーズ P 5 を経ることにより、携帯機器 3 0 の権限を変更することができる。これにより、リモートアクセスシステムにおいては、携帯機器 3 0 が新た

な任意の操作を行うことが可能となる。

【 0 1 4 0 】

以上のように、リモートアクセスシステムは、プロシキ情報が記述された属性証明書 AC_P を用いて権限管理を行うことができる。

【 0 1 4 1 】

さて、以下では、このようなリモートアクセスシステムを具体的に適用した適用例について説明する。なお、本発明におけるリソースとは、上述したように、ログインする機器そのものを示す場合がある他、これらの機器が保持するファイル等のデータやその他の各種情報を含む概念であるが、ここでは、これらリソースの具体例についても言及する。

【 0 1 4 2 】

まず、リモートアクセスシステムの適用例としては、ホームサーバやパーソナルコンピュータ等の情報処理端末が保持するデータへのリモートアクセスを行うデータアクセスシステムがあげられる。

【 0 1 4 3 】

このデータアクセスシステムにおいては、ホームサーバや情報処理端末が保持するデータがリソースとなり、携帯機器を用いてユーザが行う操作は、データを保持するホームサーバや情報処理端末に対するデータアクセスとなる。

【 0 1 4 4 】

このようなデータアクセスシステムにおいては、ホームゲートウェイによって適切なプロシキ情報を記述した属性証明書 AC_P を携帯機器に対して発行し、携帯機器がデータにアクセスする際に、当該属性証明書 AC_P をホームゲートウェイを介してホームサーバや情報処理端末に対して提示する。これにより、データアクセスシステムにおいては、携帯機器を用いてホームゲートウェイを介してデータに対してアクセスすることが可能となる。

【 0 1 4 5 】

このように、リモートアクセスシステムは、ホームサーバやパーソナルコンピュータ等の情報処理端末が保持するデータに対するデータアクセスシステムに適用することができる。

【 0 1 4 6 】

また、リモートアクセスシステムの他の適用例としては、家電カメラを用いた画像撮影による情報取得システムがあげられる。

【 0 1 4 7 】

具体的に説明するために、例えば家庭内の冷蔵庫の在庫を情報として取得する情報取得システムを考える。この情報取得システムにおいては、冷蔵庫内部の画像がリソースとなり、携帯機器を用いてユーザが行う操作は、取得した画像を閲覧することによる冷蔵庫の在庫確認となる。

【 0 1 4 8 】

このような情報取得システムにおいては、ホームゲートウェイによって適切なプロシキ情報を記述した属性証明書 AC_P を携帯機器に対して発行し、携帯機器が家電カメラが内部に取り付けられた冷蔵庫にアクセスする際に、当該属性証明書 AC_P をホームゲートウェイを介して冷蔵庫に対して提示する。これにより、情報取得システムにおいては、ユーザが外出している最中であっても、ユーザが所持する携帯機器を用いてホームゲートウェイを介して家電カメラを操作し、冷蔵庫内部の画像を取得することが可能となる。

【 0 1 4 9 】

このように、リモートアクセスシステムは、家電カメラを用いた画像撮影による情報取得システムに適用することができる。

【 0 1 5 0 】

さらに、リモートアクセスシステムの他の適用例としては、任意の場所の画像撮影による情報取得システムがあげられる。

【 0 1 5 1 】

具体的に説明するために、例えば所定の会員である旨を証明するための会員カードの画像を取得することによって会員であるか否かを認証する情報取得システムを考える。この情報取得システムにおいては、家庭等の任意の場所にある会員カードの画像がリソースとなり、携帯機器を用いてユーザが行う操作は、会員カードの認証者に画像を閲覧させることによって会員である旨を証明するものとなる。

【 0 1 5 2 】

このような情報取得システムにおいては、ホームゲートウェイによって適切なプロシキ情報を記述した属性証明書 AC_P を携帯機器に対して発行し、携帯機器が会員カードを撮影するカメラにアクセスする際に、当該属性証明書 AC_P をホームゲートウェイを介してカメラに対して提示する。これにより、情報取得システムにおいては、会員カードがユーザの手元にない場合であっても、ユーザが所持する携帯機器を用いてホームゲートウェイを介してカメラを操作し、会員カードの画像を取得することが可能となる。

【 0 1 5 3 】

このように、リモートアクセスシステムは、任意の場所の画像撮影による情報取得システムに適用することができる。

【 0 1 5 4 】

さらにまた、リモートアクセスシステムの他の適用例としては、屋外からのリモート操作による家電操作を行う家電操作システムがあげられる。

【 0 1 5 5 】

具体的に説明するために、例えば家庭内のエアーコンディショナ機器のオン／オフ操作を行う家電操作システムを考える。この家電操作システムにおいては、エアーコンディショナ機器自体がリソースとなり、携帯機器を用いてユーザが行う操作は、このリソースとしてのエアーコンディショナ機器をリモート操作するためのリモートコントローラに対するアクセスとなる。

【 0 1 5 6 】

このような家電操作システムにおいては、ホームゲートウェイによって適切なプロシキ情報を記述した属性証明書 AC_P を携帯機器に対して発行し、携帯機器がリモートコントローラにアクセスする際に、当該属性証明書 AC_P をホームゲートウェイを介してリモートコントローラに対して提示する。これにより、家電操作システムにおいては、ユーザが外出している最中であっても、ユーザが所持する携帯機器を用いてホームゲートウェイを介してリモートコントローラを操作し、エアーコンディショナ機器のオン／オフ操作を行うことが可能となる。

【 0 1 5 7 】

このように、リモートアクセスシステムは、屋外からのリモート操作による家電操作を行う家電操作システムに適用することができる。

【 0 1 5 8 】

以上説明したように、本発明の実施の形態として示したリモートアクセスシステムは、プロシキ情報が記述された属性証明書 AC_P を用いて権限管理を行うことにより、携帯機器 30 からリソースとしての対象機器 10_1 , 10_2 のそれぞれに対してリモートアクセスを行う際に、対象機器 10_1 , 10_2 毎に、権限単位での制御を容易に行うことができる。

【 0 1 5 9 】

また、このリモートアクセスシステムは、属性証明書 AC_P を利用する際に、リソースとしての対象機器 10_1 , 10_2 のそれぞれが属するネットワークの入り口となるホームゲートウェイ 20 を経由して、対象機器 10_1 , 10_2 のそれぞれと携帯機器 30 との間で属性証明書 AC_P の授受を行うことにより、属性証明書 AC_P の送付ルートが一義に決定されることから、属性証明書 AC_P の送付ルートを確認することができ、セキュリティを向上させることができる。

【 0 1 6 0 】

なお、本発明は、上述した実施の形態に限定されるものではない。例えば、上述した実施の形態では、アクセスの対象となる対象機器 10_1 , 10_2 が属する家庭内ネットワークの入り口となるホームゲートウェイ 20 が携帯機器 30 に対して属性証明書 AC_P を発行するものとして説明したが、本発明は、属性証明書 AC_P を発行するエンティティに拘泥するものではなく、ホームゲートウェイ 20 は、少なくとも属性証明書 AC_P の内容に応じて、当該属性証明書 AC_P を適切な提示先に提示する機能を有するものであればよい。

【 0 1 6 1 】

この具体例として、あるネットワークの入り口としてのホームゲートウェイによって発行された属性証明書 AC_P を用いて、他のネットワークに属するリソースにアクセスするリモートアクセスシステムについて説明する。

【 0 1 6 2 】

このリモートアクセスシステムは、概念的には、図 16 に示すように、第 1 の

家庭内ネットワークに属する対象機器 10_1 , 10_2 と、これらの対象機器 10_1 , 10_2 が属する第1の家庭内ネットワークの入り口となるホームゲートウェイと 20_1 と、対象機器 10_1 , 10_2 に対してアクセスするためにユーザが所持する携帯機器 30_1 と、第1の家庭内ネットワークとは異なる第2の家庭内ネットワークに属する対象機器 10_3 と、この対象機器 10_3 が属する第2の家庭内ネットワークの入り口となるホームゲートウェイと 20_2 と、対象機器 10_3 に対してアクセスするために他のユーザが所持する携帯機器 30_2 と、図示しないが、上述した証明書発行認証局 CA 及び属性認証局 AA とを、エンティティとして備える。

【 0 1 6 3 】

すなわち、このリモートアクセスシステムは、第1の家庭内ネットワークから構成される図6に示したようなシステムと、他の家屋等の第2のネットワークから構成される同様のシステムとが、併存しているものである。

【 0 1 6 4 】

対象機器 10_1 , 10_2 は、それぞれ、第1の家庭内ネットワークを構成する機器であり、図示しない証明書発行認証局 CA によって発行された公開鍵証明書 PKC_{T1} , PKC_{T2} を保持し、これらの公開鍵証明書 PKC_{T1} , PKC_{T2} を用いてホームゲートウェイ 20_1 との間で相互認証を行う。また、対象機器 10_1 , 10_2 は、それぞれ、携帯機器 30_1 がアクセスする際に送信した属性証明書 AC_{P1} をホームゲートウェイ 20_1 を介して受信し、この属性証明書 AC_{P1} の検証を行う。

【 0 1 6 5 】

ホームゲートウェイ 20_1 は、対象機器 10_1 , 10_2 が属する第1の家庭内ネットワークと他のネットワークとを相互に接続するためのインターフェースとして機能する。ホームゲートウェイ 20_1 は、図示しない証明書発行認証局 CA によって発行された公開鍵証明書 PKC_{G1} を保持し、この公開鍵証明書 PKC_{G1} を用いて対象機器 10_1 , 10_2 、携帯機器 30_1 、及び図示しない属性認証局 AA との間で相互認証を行う。また、ホームゲートウェイ 20_1 は、携帯機器 30_1 に対して属性証明書 AC_{P1} を発行する許可を与えるための属性証明書

AC_{L1} が図示しない属性認証局 AA によって発行されると、この属性証明書 AC_{L1} を保持し、この属性証明書 AC_{L1} に基づいて、携帯機器 30_1 に対して属性証明書 AC_{P1} を発行する。さらに、ホームゲートウェイ 20_1 は、携帯機器 30_1 から送信された属性証明書 AC_{P1} を受信すると、この属性証明書 AC_{P1} を対象機器 10_1 、 10_2 のそれぞれに対して送信して提示する。

【0166】

さらにまた、ホームゲートウェイ 20_1 は、アクセスすることができる他のネットワークにおけるホームゲートウェイを示す情報が記述された後に詳述する属性証明書 AC_H が図示しない属性認証局 AA によって発行されると、この属性証明書 AC_H を保持し、この属性証明書 AC_H に基づいて、第2の家庭内ネットワークにおけるホームゲートウェイ 20_2 と通信を行うことが可能とされる。ホームゲートウェイ 20_1 は、この属性証明書 AC_H を第2の家庭内ネットワークにおけるホームゲートウェイ 20_2 に対して送信して提示することにより、第2の家庭内ネットワークに属する対象機器 10_3 に対するアクセス許可を得るための属性証明書 AC_{P1}' をホームゲートウェイ 20_2 によって発行してもらい、携帯機器 30_1 に対してこの属性証明書 AC_{P1}' を送信する。そして、ホームゲートウェイ 20_1 は、携帯機器 30_1 から送信された属性証明書 AC_{P1}' を受信すると、この属性証明書 AC_{P1}' を属性証明書 AC_H とともにホームゲートウェイ 20_2 に対して送信して提示する。なお、この属性証明書 AC_{P1}' については、後に詳述するものとする。

【0167】

携帯機器 30_1 は、通常は、第1の家庭内ネットワークに属する対象機器 10_1 、 10_2 のそれぞれに対してアクセスするための機器であり、インターネット等のセキュアでないネットワーク NT を介してホームゲートウェイ 20_1 に対して接続可能とされる。携帯機器 30_1 は、図示しない証明書発行認証局 CA によって発行された公開鍵証明書 PKC_{M1} を保持し、この公開鍵証明書 PKC_{M1} を用いてホームゲートウェイ 20_1 との間で相互認証を行う。携帯機器 30_1 は、リソースとしての対象機器 10_1 、 10_2 のそれぞれに対してアクセスすることを認証するための属性証明書 AC_{P1} がホームゲートウェイ 20_1 によって発

行されると、この属性証明書 AC_{P1} を IC カード等に格納すること等によって保持する。そして、携帯機器 30_1 は、対象機器 10_1 , 10_2 のそれぞれに対してアクセスしようと試みる際に、IC カード等に格納された属性証明書 AC_{P1} を用いたログイン操作を行うことにより、この属性証明書 AC_{P1} をホームゲートウェイ 20_1 に対して送信して提示する。

【0168】

また、携帯機器 30_1 は、第2の家庭内ネットワークに属する対象機器 10_3 もアクセスの対象とすることができる。このとき、携帯機器 30_1 は、リソースとしての対象機器 10_3 に対してアクセスすることを認証するための属性証明書 AC_{P1}' がホームゲートウェイ 20_2 によって発行され、ホームゲートウェイ 20_1 を介してこの属性証明書 AC_{P1}' を受信すると、この属性証明書 AC_{P1}' を IC カード等に格納すること等によって保持する。そして、携帯機器 30_1 は、対象機器 10_3 に対してアクセスしようと試みる際に、IC カード等に格納された属性証明書 AC_{P1}' を用いたログイン操作を行うことにより、この属性証明書 AC_{P1}' をホームゲートウェイ 20_1 に対して送信して提示する。

【0169】

対象機器 10_3 は、第2の家庭内ネットワークを構成する機器であり、図示しない証明書発行認証局 CA によって発行された公開鍵証明書 PKC_{T3} を保持し、この公開鍵証明書 PKC_{T3} を用いてホームゲートウェイ 20_2 との間で相互認証を行う。また、対象機器 10_3 は、携帯機器 30_2 がアクセスする際に送信した属性証明書 AC_{P2} をホームゲートウェイ 20_2 を介して受信し、この属性証明書 AC_{P2} の検証を行う。さらに、対象機器 10_3 は、携帯機器 30_1 のアクセス対象とされた場合には、当該携帯機器 30_1 がアクセスする際に送信した属性証明書 AC_{P1}' と、ホームゲートウェイ 20_1 が送信した属性証明書 AC_H とを、ホームゲートウェイ 20_2 を介して受信し、これらの属性証明書 AC_{P1}' , AC_H の検証を行う。

【0170】

ホームゲートウェイ 20_2 は、対象機器 10_3 が属する第2の家庭内ネットワークと他のネットワークとを相互に接続するためのインターフェースとして機能

する。ホームゲートウェイ 2 0₂ は、図示しない証明書発行認証局 CA によって発行された公開鍵証明書 PKC_{G 2} を保持し、この公開鍵証明書 PKC_{G 2} を用いて対象機器 1 0₃、携帯機器 3 0₂、及び図示しない属性認証局 AA との間で相互認証を行う。また、ホームゲートウェイ 2 0₂ は、携帯機器 3 0₂ に対して属性証明書 AC_{P 2} を発行する許可を与えるための属性証明書 AC_{L 2} が図示しない属性認証局 AA によって発行されると、この属性証明書 AC_{L 2} を保持し、この属性証明書 AC_{L 2} に基づいて、携帯機器 3 0₂ に対して属性証明書 AC_P を発行する。さらに、ホームゲートウェイ 2 0₂ は、携帯機器 3 0₂ から送信された属性証明書 AC_{P 2} を受信すると、この属性証明書 AC_{P 2} を対象機器 1 0₃ に対して送信して提示する。

【 0 1 7 1 】

さらにまた、ホームゲートウェイ 2 0₂ は、ホームゲートウェイ 2 0₁ から属性証明書 AC_H を受信すると、この属性証明書 AC_H に基づいて、属性証明書 AC_{P 1}' をホームゲートウェイ 2 0₁ に対して発行する。そして、ホームゲートウェイ 2 0₂ は、ホームゲートウェイ 2 0₁ を介して携帯機器 3 0₁ から送信された属性証明書 AC_{P 1}' と、ホームゲートウェイ 2 0₁ から送信された属性証明書 AC_H とを受信すると、これらの属性証明書 AC_{P 1}', AC_H 対象機器 1 0₃ に対して送信して提示する。

【 0 1 7 2 】

携帯機器 3 0₂ は、第 2 の家庭内ネットワークに属する対象機器 1 0₃ に対してアクセスするための機器であり、インターネット等のセキュアでないネットワーク NT を介してホームゲートウェイ 2 0₂ に対して接続可能とされる。携帯機器 3 0₂ は、図示しない証明書発行認証局 CA によって発行された公開鍵証明書 PKC_{M 2} を保持し、この公開鍵証明書 PKC_{M 2} を用いてホームゲートウェイ 2 0₂ との間で相互認証を行う。また、携帯機器 3 0₂ は、リソースとしての対象機器 1 0₃ に対してアクセスすることを認証するための属性証明書 AC_{P 2} がホームゲートウェイ 2 0₂ によって発行されると、この属性証明書 AC_{P 2} を IC カード等に格納すること等によって保持する。そして、携帯機器 3 0₂ は、対象機器 1 0₃ に対してアクセスしようと試みる際に、IC カード等に格納された

属性証明書 AC_{P2} を用いたログイン操作を行うことにより、この属性証明書 AC_{P2} をホームゲートウェイ 20_2 に対して送信して提示する。

【0173】

このようなりモートアクセスシステムにおいては、上述した2つの属性証明書 AC_L 、 AC_P の他、2つの属性証明書 AC_H 、 AC_{P1}' が使用される。

【0174】

まず、属性証明書 AC_H について説明する。

【0175】

属性証明書 AC_H は、上述したように、アクセスすることができる他のネットワークにおけるエンティティ、具体的にはホームゲートウェイ 20_2 を示す情報が記述されたものであり、図示しない属性認証局 AA によって署名されてホームゲートウェイ 20_1 に対して発行されるものである。例えば、この属性証明書 AC_H には、上述した属性 (attributes) における各フィールドのうち、アクセス許可情報 (Access Identity) 等を用いて、アクセスすることができる他のネットワークにおけるエンティティとしてのホームゲートウェイ 20_2 を示す情報を記述することができる。

【0176】

リモートアクセスシステムにおいては、アクセスすることができる他のネットワークにおけるエンティティとしてのホームゲートウェイ 20_2 を示す情報を記述した属性証明書 AC_H を、ホームゲートウェイ 20_1 からの要求に応じて、ホームゲートウェイ 20_2 によって発行することができる。これにより、リモートアクセスシステムにおいては、この属性証明書 AC_H を保持したホームゲートウェイ 20_1 を介して携帯機器 30_1 が対象機器 10_3 に対してアクセスすることが可能となる。

【0177】

つぎに、属性証明書 AC_{P1}' について説明する。

【0178】

属性証明書 AC_{P1}' は、上述した属性証明書 AC_P と同様に、ある公開鍵証明書を保持している機器又はユーザに対する権限が記述されたものであり、ここ

では、公開鍵証明書 PKC_{M1} を保持している携帯機器 30_1 に対する権限として、第2の家庭内ネットワークに属するリソースとしての対象機器 10_3 に対してアクセスすることを許可する旨の情報が記述されたものである。例えば、この属性証明書 AC_{P1}' は、属性 (attributes) については上述した属性証明書 AC_P と同様に、認証情報 (Service Authentication Information) やアクセス許可情報 (Access Identity) 等を用いて、アクセスする対象、アクセスできる操作 (権限)、及びアクセスするための認証情報がある場合には当該認証情報が記述される一方で、プロキシ情報 (Proxy Info) としては、当該属性証明書 AC_{P1}' を経由させる2つのホームゲートウェイ 20_1 , 20_2 を識別するためのアドレスや識別子等の情報が記述されたものとなる。

【0179】

このように、リモートアクセスシステムにおいては、携帯機器 30_1 に対する権限として、第2の家庭内ネットワークに属するリソースとしての対象機器 10_3 に対してアクセスすることを許可する旨の情報が記述されるとともに、プロキシ情報として、2つのホームゲートウェイ 20_1 , 20_2 の情報が記述された属性証明書 AC_{P1}' を、ホームゲートウェイ 20_2 からホームゲートウェイ 20_1 を介して携帯機器 30_1 に対して発行することができる。これにより、リモートアクセスシステムにおいては、対象機器 10_3 が、この属性証明書 AC_{P1}' をホームゲートウェイ 20_2 を介して受信した場合には、プロキシ情報におけるターゲットを検証し、且つ、2つのホームゲートウェイ 20_1 , 20_2 を介して受信した属性証明書であることを検証することになる。

【0180】

さて、このようなりモートアクセスシステムにおいては、具体的には、先に図11に示したように、準備フェーズP1、登録フェーズP2、アクセスフェーズP3、アクセス削除フェーズP4、及びアクセス変更フェーズP5が行われる。なお、以下では、携帯機器 30_1 によって第2の家庭内ネットワークに属する対象機器 10_3 に対してアクセスするものとして説明する。

【0181】

まず、準備フェーズP1について説明する。

【0182】

リモートアクセスシステムにおいては、当該リモートアクセスシステムを構築するための準備フェーズP1として、各エンティティが相互認証可能となるように、証明書発行認証局CAにより、各エンティティに対して認証のための公開鍵証明書を発行する。すなわち、リモートアクセスシステムにおいては、上述したように、各エンティティの製造時等に、証明書発行認証局CAにより、公開鍵証明書 PKC_{T1} 、 PKC_{T2} 、 PKC_{T3} を、それぞれ、対象機器 10_1 、 10_2 、 10_3 に対して発行するとともに、公開鍵証明書 PKC_{G1} 、 PKC_{G2} を、それぞれ、ホームゲートウェイ 20_1 、 20_2 に対して発行するとともに、公開鍵証明書 PKC_{M1} 、 PKC_{M2} を、それぞれ、携帯機器 30_1 、 30_2 に対して発行する。

【0183】

リモートアクセスシステムは、このような準備フェーズP1を経ることにより、各エンティティが相互認証可能な状態に構築される。

【0184】

つぎに、登録フェーズP2について説明する。

【0185】

リモートアクセスシステムにおいては、任意の携帯機器としての携帯機器 30 をリソースに対してアクセスする機器として登録するための登録フェーズP2として、図17に示す工程が行われる。

【0186】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップS41において、属性認証局AAにより、上述した準備フェーズP1にて証明書発行認証局CAによって発行されてホームゲートウェイ 20_1 に保持されている公開鍵証明書 PKC_{G1} を用いて、ホームゲートウェイ 20_1 との間で相互認証を行う。この相互認証は、ホームゲートウェイ 20_1 自体に対する認証であり、ホームゲートウェイ 20_1 が正当なものであるか否かを認証するためのものである。

【0187】

続いて、リモートアクセスシステムにおいては、ステップ S 4 2 において、属性認証局 A A により、ホームゲートウェイ 2 0 ₁ がユーザサイドに渡ってから初回接続時等に、携帯機器 3 0 ₁ に対して属性証明書 A C _{P 1} を発行する許可を与えるための属性証明書 A C _{L 1} を、ホームゲートウェイ 2 0 ₁ に対して発行する。この際、リモートアクセスシステムにおいては、ホームゲートウェイ 2 0 ₁ が他のホームゲートウェイ 2 0 ₂ に対してアクセスする場合には、属性認証局 A A により、ホームゲートウェイ 2 0 ₂ に対してアクセスできる旨の情報が記述された属性証明書 A C _H を、ホームゲートウェイ 2 0 ₁ に対して発行する。これにともない、ホームゲートウェイ 2 0 ₁ は、属性認証局 A A から送信された 2 つの属性証明書 A C _{L 1} , A C _H を保持する。

【 0 1 8 8 】

続いて、リモートアクセスシステムにおいては、ステップ S 4 3 において、ホームゲートウェイ 2 0 ₁ により、ユーザからの指示にしたがい、接続する機器、すなわち、対象機器 1 0 ₁ , 1 0 ₂ のそれぞれの情報を登録するとともに、その対象機器 1 0 ₁ , 1 0 ₂ のそれぞれに対してリモートからアクセスしてもよい携帯機器 3 0 ₁ に対して上述したプロシキ情報を記述した属性証明書 A C _{P 1} を発行する。

【 0 1 8 9 】

続いて、リモートアクセスシステムにおいては、携帯機器 3 0 ₁ から他のホームゲートウェイ 2 0 ₂ を介して対象機器 1 0 ₃ に対してアクセスしたい場合には、ステップ S 4 4 において、ホームゲートウェイ 2 0 ₁ により、保持している属性証明書 A C _H を他のホームゲートウェイ 2 0 ₂ に対して送信して提示し、上述したプロシキ情報を記述した属性証明書 A C _{P 1} ' を発行してもらう。これにともない、ホームゲートウェイ 2 0 ₂ は、属性証明書 A C _{P 1} ' を発行し、この属性証明書 A C _{P 1} ' をホームゲートウェイ 2 0 ₁ に対して送信する。

【 0 1 9 0 】

続いて、リモートアクセスシステムにおいては、ステップ S 4 5 において、携帯機器 3 0 ₁ により、上述した準備フェーズ P 1 にて証明書発行認証局 C A によって発行されて保持している公開鍵証明書 P K C _{M 1} を用いて、ホームゲートウ

エイ 2 0₁ との間で相互認証を行う。

【 0 1 9 1 】

そして、リモートアクセスシステムにおいては、ステップ S 4 6 において、携帯機器 3 0₁ により、ホームゲートウェイ 2 0₁ から送信された属性証明書 A C_{P 1}, A C_{P 1}' を I C カード等に格納して保持し、一連の登録フェーズ P 2 を終了する。

【 0 1 9 2 】

リモートアクセスシステムにおいては、このような一連の工程からなる登録フェーズ P 2 を経ることにより、リソースに対してアクセスする機器として、携帯機器 3 0₁ を登録することができる。このようにしてリソースに対してアクセスする携帯機器 3 0₁ の登録がされたリモートアクセスシステムにおいては、登録された携帯機器 3 0₁ が任意の操作を行うことが可能となる。

【 0 1 9 3 】

つぎに、アクセスフェーズ P 3 について説明する。

【 0 1 9 4 】

リモートアクセスシステムにおいては、登録された携帯機器 3 0₁ がリソースに対してアクセスする際には、アクセスフェーズ P 3 として、図 1 8 に示す工程が行われる。

【 0 1 9 5 】

まず、リモートアクセスシステムにおいては、同図に示すように、ステップ S 5 1 において、携帯機器 3 0₁ により、保持している公開鍵証明書 P K C_{M 1} を用いて、ホームゲートウェイ 2 0₁ との間で相互認証を行う。

【 0 1 9 6 】

続いて、リモートアクセスシステムにおいては、ステップ S 5 2 において、携帯機器 3 0₁ により、保持している属性証明書 A C_{P 1}, A C_{P 1}' のいずれかをホームゲートウェイ 2 0₁ に対して送信して提示する。具体的には、リモートアクセスシステムにおいては、対象機器 1 0₁, 1 0₂ のいずれか又は双方に対してアクセスする場合には、携帯機器 3 0₁ により、保持している属性証明書 A C_{P 1} をホームゲートウェイ 2 0₁ に対して送信して提示する一方で、対象機器

10₃ に対してアクセスする場合には、携帯機器 30₁ により、保持している属性証明書 AC_{P1}' をホームゲートウェイ 20₁ に対して送信して提示する。

【0197】

ここで、リモートアクセスシステムにおいては、携帯機器 30₁ により、保持している属性証明書 AC_{P1} をホームゲートウェイ 20₁ に対して送信して提示した場合には、先に図 13 中ステップ S13 乃至ステップ S17 に示した処理と同様の処理を行うが、ここでは、携帯機器 30₁ は、保持している属性証明書 AC_{P1}' をホームゲートウェイ 20₁ に対して送信して提示するものとして説明する。

【0198】

リモートアクセスシステムにおいては、ステップ S53 において、ホームゲートウェイ 20₁ により、携帯機器 30₁ から提示された属性証明書 AC_{P1}' におけるプロシキ情報を検証し、アクセス対象の機器が自己の配下にある第 1 の家庭内ネットワークとは異なる第 2 の家庭内ネットワークに属する対象機器 10₃ である旨を把握すると、2 つの属性証明書 AC_{P1}'、AC_H を、第 2 の家庭内ネットワークを司るホームゲートウェイ 20₂ に対して送信して提示する。

【0199】

続いて、リモートアクセスシステムにおいては、ステップ S54 において、ホームゲートウェイ 20₂ により、ホームゲートウェイ 20₁ から提示された 2 つの属性証明書 AC_{P1}'、AC_H の内容に基づいて、当該属性証明書 AC_{P1}'、AC_H を、アクセスする対象として指定された機器、すなわち、対象機器 10₃ に対して送信して提示する。

【0200】

続いて、リモートアクセスシステムにおいては、ステップ S55 において、対象機器 10₃ により、ホームゲートウェイ 20₂ から送信された 2 つの属性証明書 AC_{P1}'、AC_H を受信し、上述したプロシキ情報や属性といった当該属性証明書 AC_{P1}'、AC_H の内容を検証する。

【0201】

リモートアクセスシステムにおいては、ステップ S56 において、属性証明書

AC_{P1}' , AC_H の検証結果が正当なものであった場合には、ステップ S 5 7 において、対象機器 1 0 3 によって携帯機器 3 0 1 のアクセスを許可し、一連のアクセスフェーズ P 3 を終了する。一方、リモートアクセスシステムにおいては、ステップ S 5 6 において、属性証明書 AC_{P1}' , AC_H の検証結果が不当なものであった場合には、ステップ S 5 8 において、対象機器 1 0 3 によって携帯機器 3 0 1 のアクセスを拒否し、一連のアクセスフェーズ P 3 を終了する。

【 0 2 0 2 】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセスフェーズ P 3 を経ることにより、対象機器 1 0 3 によって携帯機器 3 0 1 の権限を判別することができ、アクセスが許可された携帯機器 3 0 1 は、任意の操作を行うことが可能となる。

【 0 2 0 3 】

つぎに、アクセス削除フェーズ P 4 について説明する。

【 0 2 0 4 】

リモートアクセスシステムにおいては、任意の携帯機器をリソースに対してアクセスする機器から除外したい場合には、アクセス削除フェーズ P 4 として、図 1 9 に示す工程が行われる。なお、リモートアクセスシステムにおいては、携帯機器 3 0 1 が対象機器 1 0 1, 1 0 2 をアクセス対象としている場合には、先に図 1 4 に示した処理と同様の処理を行えばよく、ここでは、携帯機器 3 0 1 が対象機器 1 0 3 をアクセス対象としており、携帯機器 3 0 1 を対象機器 1 0 3 に対してアクセスする機器から除外したい場合について説明する。

【 0 2 0 5 】

まず、リモートアクセスシステムにおいては、図 1 9 に示すように、ステップ S 6 1 において、ホームゲートウェイ 2 0 1 により、ユーザからの指示にしたがい、対象機器 1 0 3 に対してリモートからアクセスしてもよい携帯機器 3 0 1 に対して発行した属性証明書 AC_{P1}' に対する CRL (ACRL) の作成をホームゲートウェイ 2 0 2 に対して要求する。

【 0 2 0 6 】

続いて、リモートアクセスシステムにおいては、ステップ S 6 2 において、ホ

ームゲートウェイ 2 0₂ により、ホームゲートウェイ 2 0₁ からの要求にしたがい、属性証明書 AC_{P1}' に対する CRL (ACRL) を作成する。

【 0 2 0 7 】

そして、リモートアクセスシステムにおいては、ステップ S 6 3 において、ホームゲートウェイ 2 0₂ により、作成した属性証明書 AC_{P1}' に対する CRL (ACRL) をホームゲートウェイ 2 0₁ に対して送信して配布する。これにともない、ホームゲートウェイ 2 0₁ は、ホームゲートウェイ 2 0₂ から送信された属性証明書 AC_{P1}' に対する CRL (ACRL) を保持する。

【 0 2 0 8 】

このように、リモートアクセスシステムにおいては、属性証明書 AC_{P1}' に対する CRL (ACRL) をホームゲートウェイ 2 0₂ によって作成することにより、携帯機器 3 0₁ からホームゲートウェイ 2 0₁ を介して対象機器 1 0₃ に対してアクセスがあった場合には、ホームゲートウェイ 2 0₁ によってアクセスを拒否することができ、携帯機器 3 0₁ をリソースに対してアクセスする機器から除外することができる。

【 0 2 0 9 】

また、リモートアクセスシステムにおいては、上述したように、正当なユーザが自らの意思で携帯機器 3 0 をリソースに対してアクセスする機器から除外したい場合等には、ステップ S 6 3 の処理に続いて、先に図 1 4 中ステップ S 2 2 乃至ステップ S 2 4 に示した処理と同様の処理を行うようにしてもよい。

【 0 2 1 0 】

すなわち、リモートアクセスシステムにおいては、ステップ S 6 4 において、携帯機器 3 0₁ により、保持している公開鍵証明書 PKC_{M1} を用いて、ホームゲートウェイ 2 0₁ との間で相互認証を行う。

【 0 2 1 1 】

続いて、リモートアクセスシステムにおいては、ステップ S 6 5 において、ホームゲートウェイ 2 0₁ からの指示にしたがい、携帯機器 3 0₁ により、保持している属性証明書 AC_{P1}' を削除する。

【 0 2 1 2 】

そして、リモートアクセスシステムにおいては、ステップS66において、ホームゲートウェイ20₁により、ステップS63にて保持したCRL（ACRL）を削除し、一連のアクセス削除フェーズP4を終了する。

【0213】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセス削除フェーズP4を経ることにより、携帯機器30₁をリソースとしての対象機器10₃に対してアクセスする機器から除外することができる。

【0214】

なお、リモートアクセスシステムにおいては、対象機器10₃の側の都合により、携帯機器30₁を当該対象機器10₃に対してアクセスする機器から除外したい場合には、ステップS61の処理をスキップし、ユーザからの指示にしたがい、ステップS62からの処理を行えばよいことになる。

【0215】

最後に、アクセス変更フェーズP5について説明する。

【0216】

リモートアクセスシステムにおいては、任意の携帯機器の権限を変更したい場合には、アクセス変更フェーズP5として、図20に示す工程が行われる。なお、リモートアクセスシステムにおいては、第1の家庭内ネットワークにおけるリソースに対する携帯機器30₁の権限を変更したい場合には、先に図15に示した処理と同様の処理を行えばよく、ここでは、第2の家庭内ネットワークにおけるリソースに対する携帯機器30₁の権限を変更したい場合について説明する。

【0217】

まず、リモートアクセスシステムにおいては、図20に示すように、ステップS71において、ホームゲートウェイ20₁により、ユーザからの指示にしたがい、保持している属性証明書AC_Hを他のホームゲートウェイ20₂に対して送信して提示し、プロシキ情報を記述した新たな属性証明書AC_{P1}'を発行してもらう。これにともない、ホームゲートウェイ20₂は、新たな属性証明書AC_{P1}'を発行し、この属性証明書AC_{P1}'をホームゲートウェイ20₁に対して送信する。

【 0 2 1 8 】

続いて、リモートアクセスシステムにおいては、ステップ S 7 2 において、携帯機器 3 0 ₁ により、保持している公開鍵証明書 P K C _{M 1} を用いて、ホームゲートウェイ 2 0 ₁ との間で相互認証を行う。

【 0 2 1 9 】

そして、リモートアクセスシステムにおいては、ステップ S 7 3 において、携帯機器 3 0 ₁ により、ホームゲートウェイ 2 0 ₁ から送信された新たな属性証明書 A C _{P 1} ' を、元の属性証明書 A C _{P 1} ' と置換して I C カード等に格納して保持し、一連のアクセス変更フェーズ P 5 を終了する。

【 0 2 2 0 】

リモートアクセスシステムにおいては、このような一連の工程からなるアクセス変更フェーズ P 5 を経ることにより、携帯機器 3 0 ₁ の権限を変更することができる。これにより、リモートアクセスシステムにおいては、携帯機器 3 0 ₁ が新たな任意の操作を行うことが可能となる。

【 0 2 2 1 】

以上のように、リモートアクセスシステムは、プロシキ情報が記述された属性証明書 A C _{P 1} ' を用いて、通常では携帯機器 3 0 ₁ からはアクセスすることができない第 2 の家庭内ネットワークにおけるリソースに対する権限管理を行うことができる。

【 0 2 2 2 】

このように、本発明は、携帯機器が通常アクセスできるネットワークの入り口としてのホームゲートウェイが当該携帯機器に対して属性証明書 A C _P を発行するのではなく、他のネットワークの入り口としてのホームゲートウェイといった任意のエンティティが属性証明書 A C _P を発行するものであってもよく、ホームゲートウェイは、属性証明書 A C _P の内容を検証できるものであればよい。

【 0 2 2 3 】

また、上述した実施の形態では、家庭内ネットワークにおけるリソースに対してアクセスするものとして説明したが、本発明は、任意のネットワークに対して適用することができる。

【 0 2 2 4 】

さらに、上述した実施の形態では、リソースに対してアクセス機器として携帯機器を用いて説明したが、本発明は、このような機器としては、携帯型の機器に限らずいかなる機器をも適用することができる。

【 0 2 2 5 】

さらにまた、本発明は、各エンティティの動作をハードウェアで実現するのみならず、ソフトウェアで実現することもできる。本発明は、ソフトウェアで実現する場合には、例えば各エンティティが備えるCPU (Central Processing Unit) によって上述したリモートアクセスを行うためのリモートアクセスプログラムを実行することにより、各機能を実現することができる。このリモートアクセスプログラムは、例えばいわゆるコンパクトディスク (Compact Disc) 等の所定の記録媒体やインターネット等の伝送媒体によって提供することができる。

【 0 2 2 6 】

このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【 0 2 2 7 】

【発明の効果】

以上詳細に説明したように、本発明にかかるリモートアクセスシステムは、所定のリソースに対して遠隔地からアクセスするリモートアクセスシステムであって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器と、このアクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入りに相当する機器であるゲートウェイ機器と、少なくともリソースに対する権限が記述された電子証明書であり、且つ、この電子証明書を経由させるゲートウェイ機器の情報が記述された電子証明書である権限及び経路情報記述属性証明書を保持し、アクセス対象機器に対してアクセスするアクセス機器とを備え、アクセス機器は、権限及び経路情報記述属性証明書をゲートウェイ機器に対して送信して提示し、ゲートウェイ機器は、アクセス機器から受信した権限及び経路情報記述属性証明書の内容を検証し、当該権限及び経路情報記述属性証明書をアクセスの対

象として指定されたアクセス対象機器に対して送信して提示し、アクセス対象機器は、ゲートウェイ機器から受信した権限及び経路情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否する。

【 0 2 2 8 】

したがって、本発明にかかるリモートアクセスシステムは、少なくともリソースに対する権限とゲートウェイ機器の情報を、権限及び経路情報記述属性証明書に記述し、この権限及び経路情報記述属性証明書を、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示し、リソースに対するアクセス機器のアクセスを検証することにより、リソース毎に、権限単位での制御を容易に行うことができ、また、権限及び経路情報記述属性証明書の送付ルートを確認することができ、セキュリティを向上させることができる。

【 0 2 2 9 】

また、本発明にかかるリモートアクセス方法は、所定のリソースに対して遠隔地からアクセスするリモートアクセス方法であって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を經由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経路情報記述属性証明書を保持させ、アクセス機器によって権限及び経路情報記述属性証明書をゲートウェイ機器に対して送信して提示し、ゲートウェイ機器によってアクセス機器から受信した権限及び経路情報記述属性証明書の内容を検証し、当該権限及び経路情報記述属性証明書をアクセスの対象として指定されたアクセス対象機器に対して送信して提示し、アクセス対象機器によってゲートウェイ機器から受信した権限及び経路情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否する。

【 0 2 3 0 】

したがって、本発明にかかるリモートアクセス方法は、少なくともリソースに

対する権限とゲートウェイ機器の情報とを、権限及び経路情報記述属性証明書に記述し、この権限及び経路情報記述属性証明書を、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示し、リソースに対するアクセス機器のアクセスを検証することにより、リソース毎に、権限単位での制御を容易に行うことが可能となり、また、権限及び経路情報記述属性証明書の送付ルートを確認することができ、セキュリティを向上させることが可能となる。

【 0 2 3 1 】

さらに、本発明にかかるリモートアクセスプログラムは、所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能リモートアクセスプログラムであって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入り口に相当し、この電子証明書を經由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経路情報記述属性証明書が保持されており、アクセス機器からゲートウェイ機器を介して送信されて提示された権限及び経路情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否する。

【 0 2 3 2 】

したがって、本発明にかかるリモートアクセスプログラムは、少なくともリソースに対する権限とゲートウェイ機器の情報とが、権限及び経路情報記述属性証明書に記述されており、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示された権限及び経路情報記述属性証明書に基づいて、リソースに対するアクセス機器のアクセスを検証することにより、このリモートアクセスプログラムが実装された機器が、リソース毎に、権限単位での制御を容易に行うことを可能とし、また、権限及び経路情報記述属性証明書の送付ルートを確認することを可能とし、セキュリティを向上させることを可能とする。

【 0 2 3 3 】

さらにまた、本発明にかかるリモートアクセスプログラムが記録された記録媒

体は、所定のリソースに対して遠隔地からアクセスするコンピュータ実行可能なリモートアクセスプログラムが記録された記録媒体であって、アクセスの対象となるリソース自体としての機器、又はリソースを保持する機器であるアクセス対象機器に対してアクセスするアクセス機器に、少なくともリソースに対する権限が記述された電子証明書であり、且つ、アクセス対象機器が属するネットワークと他のネットワークとを相互に接続することを可能とするネットワークの入りに相当し、この電子証明書を経由させる機器であるゲートウェイ機器の情報が記述された電子証明書である権限及び経路情報記述属性証明書が保持されており、リモートアクセスプログラムは、アクセス機器からゲートウェイ機器を介して送信されて提示された権限及び経路情報記述属性証明書の内容を検証し、リソースに対するアクセス機器のアクセスを許可又は拒否する。

【 0 2 3 4 】

したがって、本発明にかかるリモートアクセスプログラムが記録された記録媒体は、少なくともリソースに対する権限とゲートウェイ機器の情報とが、権限及び経路情報記述属性証明書に記述されており、アクセス機器からアクセス対象機器に対してゲートウェイ機器を介して送信して提示された権限及び経路情報記述属性証明書に基づいて、リソースに対するアクセス機器のアクセスを検証するリモートアクセスプログラムを提供することができる。そのため、このリモートアクセスプログラムが実装された機器は、リソース毎に、権限単位での制御を容易に行うことができ、また、権限及び経路情報記述属性証明書の送付ルートを確認することができ、セキュリティを向上させることができる。

【図面の簡単な説明】

【図 1】

公開鍵証明書のフォーマットを説明する図である。

【図 2】

公開鍵証明書のフォーマットを説明する図であって、図 1 に示す項目に続く残りの項目を説明する図である。

【図 3】

属性証明書のフォーマットを説明する図である。

【図 4】

属性証明書のフォーマットを説明する図であって、図 3 に示す項目に続く残りの項目を説明する図である。

【図 5】

権限プロキシ機能を説明するための図である。

【図 6】

本発明の実施の形態として示すリモートアクセスシステムの概念図である。

【図 7】

図 4 に示す属性証明書の項目のうち、属性における各フィールドの抜粋を示す図である。

【図 8】

ロールの概念を用いた権限管理の手法について説明する図である。

【図 9】

図 4 に示す属性証明書の項目のうち、拡張情報における各フィールドの抜粋を示す図である。

【図 10】

図 4 に示す属性証明書の項目のうち、拡張情報におけるプロキシ情報の具体的な記述内容を説明する図である。

【図 11】

同リモートアクセスシステムにて行われる各フェーズを説明するためのフローチャートである。

【図 12】

同リモートアクセスシステムにおける登録フェーズとしての一連の工程を説明するためのフローチャートである。

【図 13】

同リモートアクセスシステムにおけるアクセスフェーズとしての一連の工程を説明するためのフローチャートである。

【図 14】

同リモートアクセスシステムにおけるアクセス削除フェーズとしての一連の工

程を説明するためのフローチャートである。

【図 15】

同リモートアクセスシステムにおけるアクセス変更フェーズとしての一連の工程を説明するためのフローチャートである。

【図 16】

本発明の他の実施の形態として示すリモートアクセスシステムの概念図である。

【図 17】

同リモートアクセスシステムにおける登録フェーズとしての一連の工程を説明するためのフローチャートである。

【図 18】

同リモートアクセスシステムにおけるアクセスフェーズとしての一連の工程を説明するためのフローチャートである。

【図 19】

同リモートアクセスシステムにおけるアクセス削除フェーズとしての一連の工程を説明するためのフローチャートであって、携帯機器を他のネットワークに属する対象機器に対してアクセスする機器から除外する場合における一連の工程を説明するためのフローチャートである。

【図 20】

同リモートアクセスシステムにおけるアクセス変更フェーズとしての一連の工程を説明するためのフローチャートであって、他のネットワークにおけるリソースに対する携帯機器の権限を変更する場合における一連の工程を説明するためのフローチャートである。

【符号の説明】

10₁, 10₂, 10₃ 対象機器、 20, 20₁, 20₂ ホームゲートウェイ、 30, 30₁, 30₂ 携帯機器、 AA 属性認証局、 AC, AC_H, AC_L, AC_{L1}, AC_{L2}, AC_P, AC_{P1}, AC_{P2}, AC_{P1}' 属性証明書、 AS 権限主張側サーバ、 AU₁₁, AU₁₂, ..., AU₂₁, AU₂₂, ... 権限、 CA 証明書発行認証局、 CL クライ

アント、 M_1, M_2, M_3 個人、NT ネットワーク、 $PKC_G, PKC_{G1}, PKC_{G2}, PKC_M, PKC_{M1}, PKC_{M2}, PKC_{T1}, PKC_{T2}, PKC_{T3}$ 公開鍵証明書、 R_1, R_2 ロール、RA 役割認証局、RAAC 役割割当証明書、RSAC 役割定義証明書、VR 権限検証側サーバ

【書類名】 図面

【図 1】

項目	説明
Version 1	
version	証明書のフォーマットのバージョン
serial Number	証明書発行認証局によって設定される証明書のシリアルナンバー
signature algorithm Identifier algorithm parameters	証明書の署名アルゴリズム、及びそのパラメータ
issuer	証明書発行認証局の名称 (Distinguished Name形式)
validity not Before not After	証明書の有効期限 開始日時 終了日時
subject	ユーザを識別する名前
subject Public Key Info algorithm subject Public key	ユーザの公開鍵情報 鍵アルゴリズム 鍵情報
Version 3	
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	証明書発行認証局の署名 確認用の鍵識別 鍵識別番号 (8進数) 証明書発行認証局の名称 (General Name形式) 認証番号
subject key Identifier	複数の鍵の証明をする場合の各鍵の識別子
key usage (0) digital Signature (1) non Repudiation (2) key Encipherment (3) data Encipherment (4) key Agreement (5) key Cert Sign (6) CRL Sign (7) encipher Only (8) decipher Only	鍵の使用目的を指定 (0) デジタル署名用 (1) 否認防止用 (2) 鍵の暗号化用 (3) メッセージの暗号化用 (4) 共通鍵配送用 (5) 認証の署名確認用 (6) 失効リストの署名確認用 (7) 鍵交換時データの暗号化にのみ利用 (8) 鍵交換時データの復号にのみ利用
private Key Usage Period not Before not After	ユーザに格納されている秘密鍵の有効期限

公開鍵証明書のフォーマットの説明図

【図 2】

Certificate Policy policy Identifier policy Qualifiers	証明書発行認証局の 証明書発行ポリシー ポリシーID 認証基準
policy Mappings Issuer Domain Policy subject Domain Policy	証明書発行認証局を認証 する場合にのみ必要。証 明書発行認証局のポリシ ーと被認証ポリシーとの マッピングを規定。
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	ディレクトリ (X.500) の アトリビュートを定義。 コミュニケーションの相手 がディレクトリ情報を利用 する場合に、事前にそのア トリビュートを知らせるの に用いる。
subject Alt Name	ユーザの別名 (GN形式)
issuer Alt Name	証明書発行者の別名
subject Directory Attributes	ユーザの任意の属性
basic Constraints CA path Len Constraint	証明対象の公開鍵が証明 書発行認証局の署名用か、 ユーザのものかを区別
name Constraints permitted Subtrees base minimum maximum excluded Subtrees	被認証者が証明書発行 認証局である場合 (CA認 証) にのみ使用
policy Constraints require Explicit Policy inhibit Policy Mapping	認証パスの残りに対する 明確な認証ポリシーID、 禁止ポリシーマップを要 求する制限を記述
CRL Distribution Points	ユーザが証明書を利用する 際に、証明書が失効してい ないかどうかを確認するた めの失効リストの参照ポイ ントを記述
署名	発行者の署名

公開鍵証明書のフォーマットの説明図

【図 3】

項目	AttributeCertificateInfo	説明
acinfo		
version	AttCertVersion	属性証明書のフォーマットのバージョン
holder	Holder	属性証明書が結び付けられた公開鍵証明書の所有者を特定
	baseCertificateID	
	issuerSerial	属性証明書の所有者の公開鍵証明書の発行番号
	issuer	
	serial	属性証明書の所有者の公開鍵証明書のシリアル番号
	issuerUID	属性証明書の所有者の公開鍵証明書の発行番号固有識別子
	entityName	属性証明書の所有者の名称
	objectDigestInfo	将来、属性証明書が識別情報や公開鍵証明書にリンクされて いない場合を想定
	objectDigestInfo	
	objectDigestInfo	
	otherObjectTypeID	
	digestAlgorithm	
	objectDigest	
issuer	AttCertIssuer	属性証明書に署名した発行者の名称を指定
	v2Form	
	issuerName	属性証明書の発行番号
	baseCertificateID	
	objectDigestInfo	
signature	AlgorithmIdentifier	属性証明書の署名を有効にするために使用するアルゴリズム 識別子
serialNumber	CertificateSerialNumber	属性証明書が各証明書に割り振るシリアルナンバ
attrCertValidityPeriod	AttCertValidityPeriod	属性証明書の有効期限
	notBefore	開始日時
	notAfter	終了日時

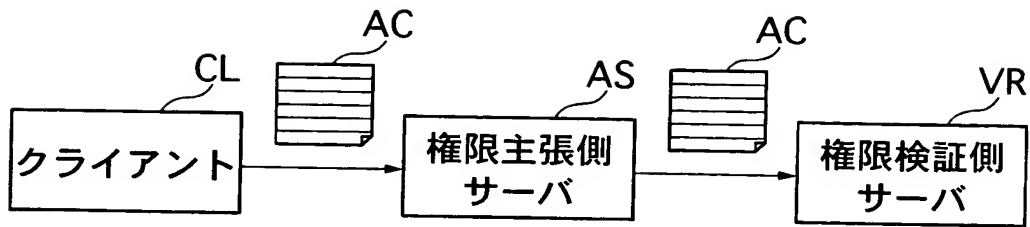
属性証明書のフォーマットの説明図

【図4】

attributes		Attribute type	AttributeType	属性証明書の所有者の特権に関する情報	
			Service Authentication service	サービスに関する認証情報を記述。属性証明書の発行者が所有者を認証する場合に利用。	
			ident		
			authInfo		
			Access Identity	属性証明書の発行者が用いる所有者のアクセス許可情報	
			Charging Identity	料金のために属性証明書の所有者を特定するための情報	
			Group	属性証明書の所有者のグループへの所属関係	
			Role	属性証明書の所有者に与えられる役割	
			roleAuthority		
			roleName		
			Clearance	属性証明書の所有者に対する秘密情報の使用許可に関する情報	
			policyId		
			classList		
			securityCategories		
		values			
	issuerUniqueID	uniqueIdentifier		属性証明書の発行者の公開鍵証明書で指定されている場合	
	extensions			利用	
			Audit Identity	属性証明書の所有者の情報はなく属性証明書の情報を記述	
			AC Targeting	サービス管理者が属性証明書の所有者の監査を行	
			Authority Key Identifier	不正行為の検出(特定)をするために用いる	
			Authority Information	属性証明書が対象とするサービスパスを記述	
			Access Points	属性証明書の発行者の鍵情報	
			No Revocation Available	OCSPレスポンスのURI	
			Proxy Info	CRL配布点のURI	
	AlgorithmIdentifier			当該属性証明書に対応する失効情報がないことを示す	
signature				属性証明書を提出できるエンティティ	
Algorithm					
signature					
Value					
Optional Features				属性証明局によってつけられた署名	

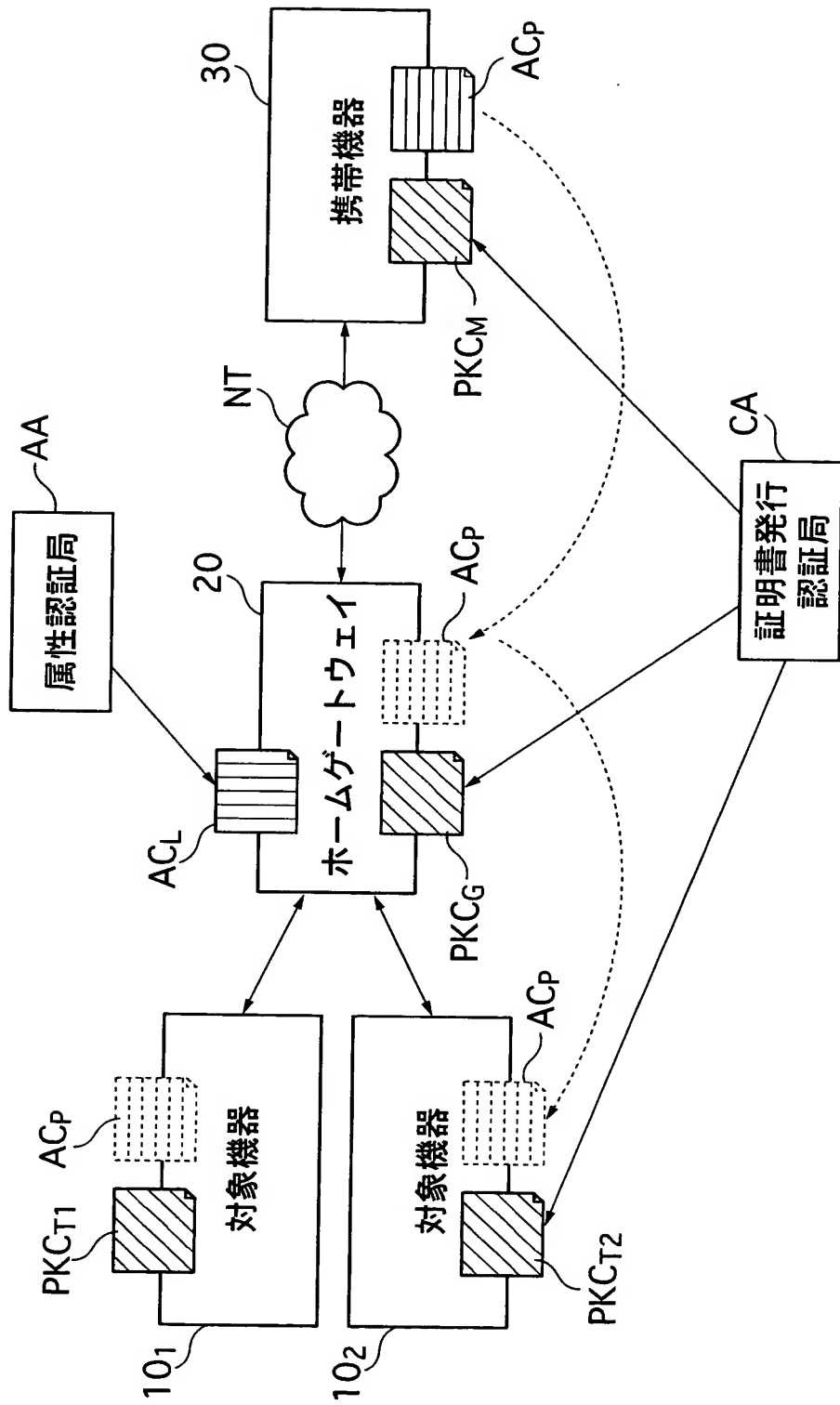
属性証明書のフォーマットの説明図

【図 5】



権限プロキシ機能の説明図

【図 6】



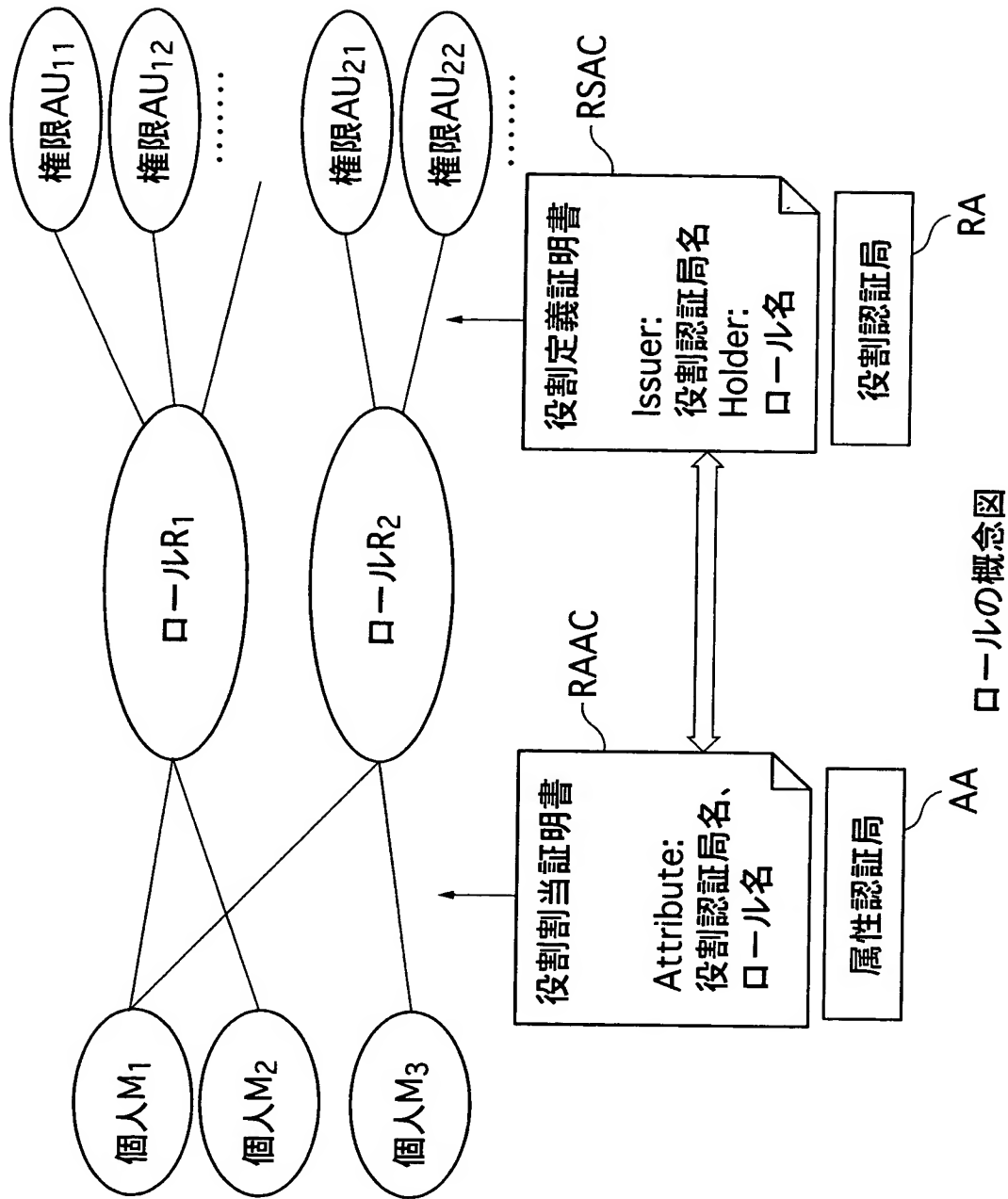
リモートアクセスシステムの構成図

【図 7】

項目	OID	値
Service Authentication Information	id-aca 1	サービス又は認証時に必要とされる情報
Access Identity	id-aca 2	所有者の属性を検証する際に所有者を識別するもの
Charging Identity	id-aca 3	サービスの課金に利用するID
Group	id-aca 4	所有者が所属するグループ情報
Role	id-at 72	役割認証局名、ロール名

属性証明書のフォーマットの説明図

【図 8】



【図 9】

項目	OID	値
Authority Information Access		属性証明書が発行者情報、OCSP情報
Authority Key Identifier		属性認証局の公開鍵情報
CRL Distribution Points		CRL配布点のURI
Audit Identity		監査用の属性証明書所有者ID(ログ追跡に用いる;匿名性があるが属性認証局にある情報を合わせれば本人の特定ができる)
Time Specification		権限が有効な時間帯
Targeting Information		属性証明書を受け取れるサーバ名
Proxy Info		可能なプロキシ
User Notice		権限所有者や権限検証者への伝達情報
権限ポリシー		policy authority名、文字列又はOIDの値
SOA (Source of Authority; 検証者が信頼するエンティティ、PKIでのルートCA, Trust anchorに相当するDelegation(属性認証局のChain)でのトップ(通常、属性認証局は1つなので、属性認証局=SOA))		SOAになれる権限 SOAの証明書である旨の記述
権限委譲		権限を他のエンティティに委譲する際の委譲条件等の記述
属性の廃棄		CRL配布点のURI
		失効をサポートしていない旨の記述
Role		役割定義証明書を示す(Role authority名、ロール名を文字列で)

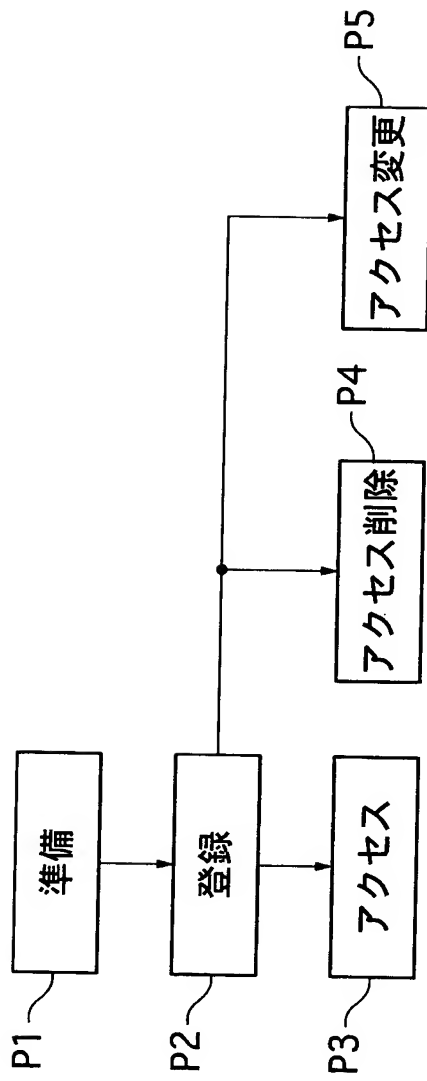
属性証明書のフォーマットの説明図

【図 10】

OID id-pe 10 }	値 1.3.6.1.5.5.7.1.10
ProxyInfo :: SEQUENCE OF Targets	
Target :: CHOICE {	
targetName[0] GeneralName,	例: ホームゲートウェイアドレス
targetGroup[1] GeneralName,	又は識別子
targetCert[2] TargetCert	例: ホームゲートウェイの公開鍵証明書
}	
TargetCert :: SEQUENCE {	
targetCertificate IssuerSerial,	
targetName GeneralName OPTIONAL,	
certDigestInfo ObjectDigestInfo OPTIONAL	
}	

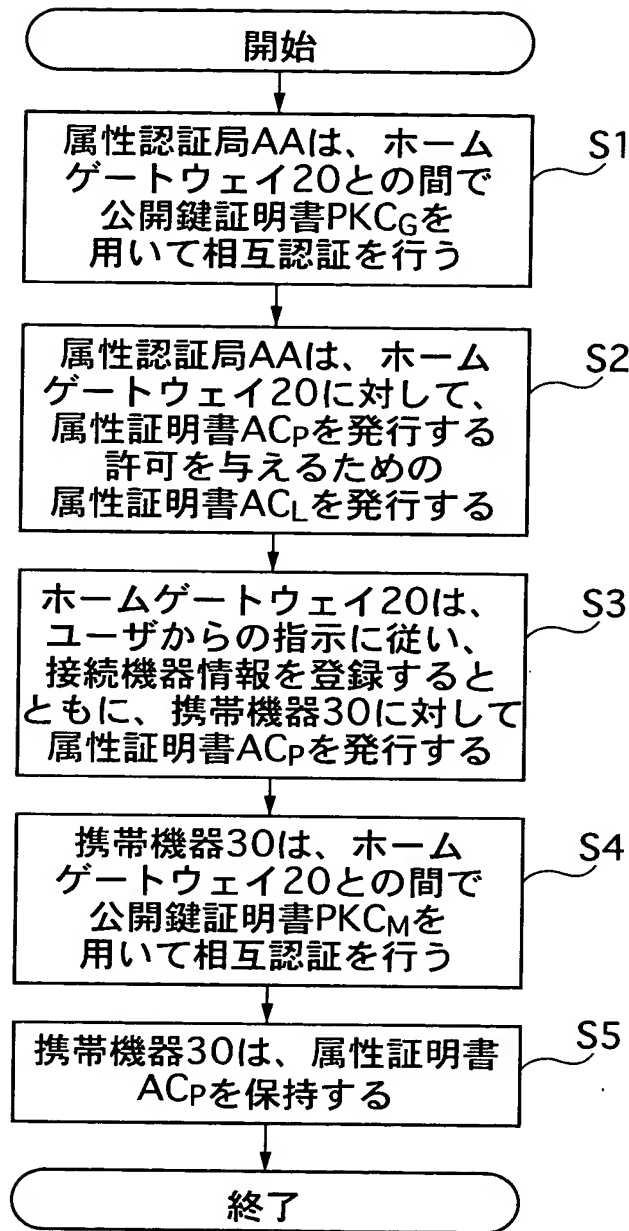
プロシキ情報の内容

【図 1 1】



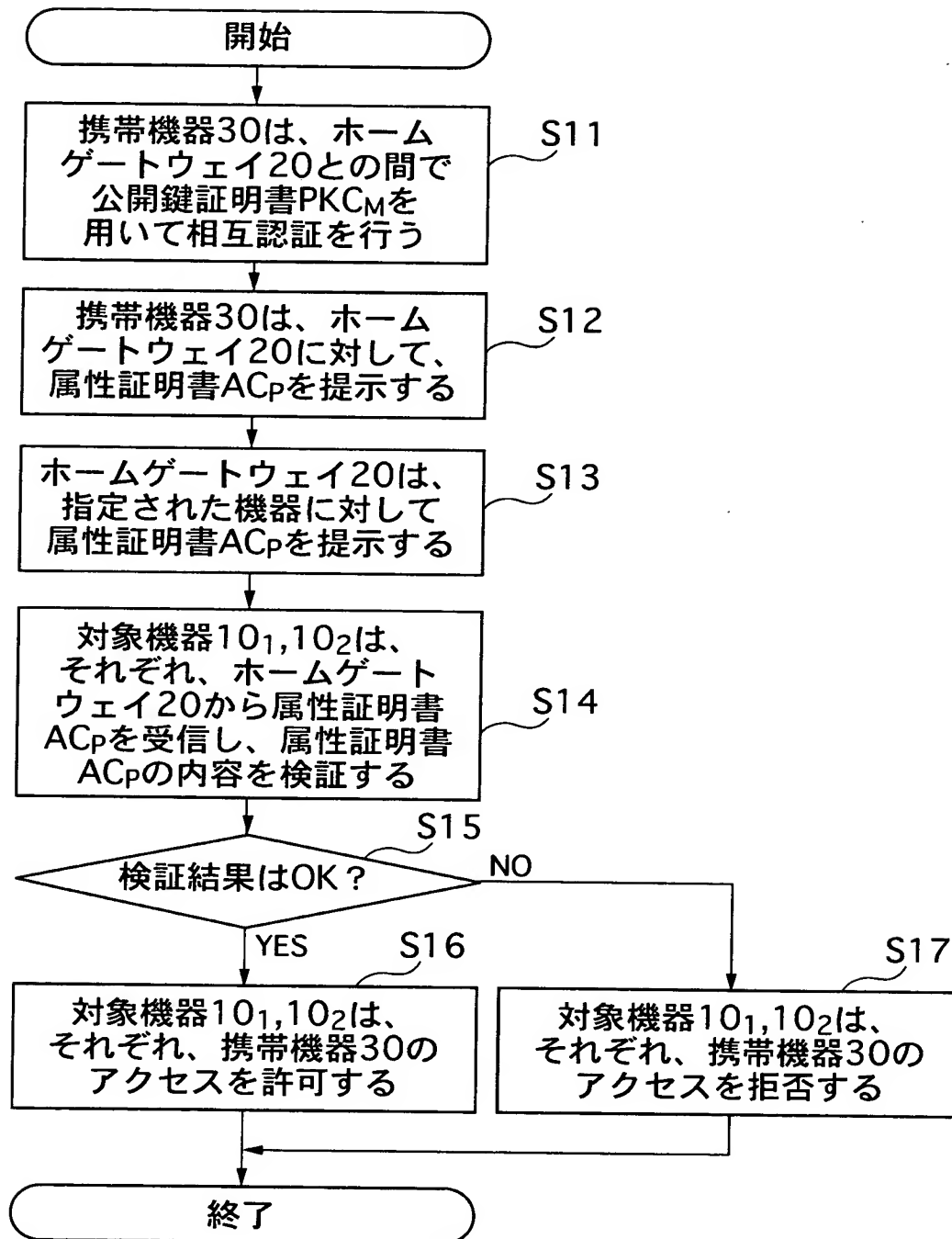
リモートアクセスシステムにおける一連の処理工程

【図 1 2】



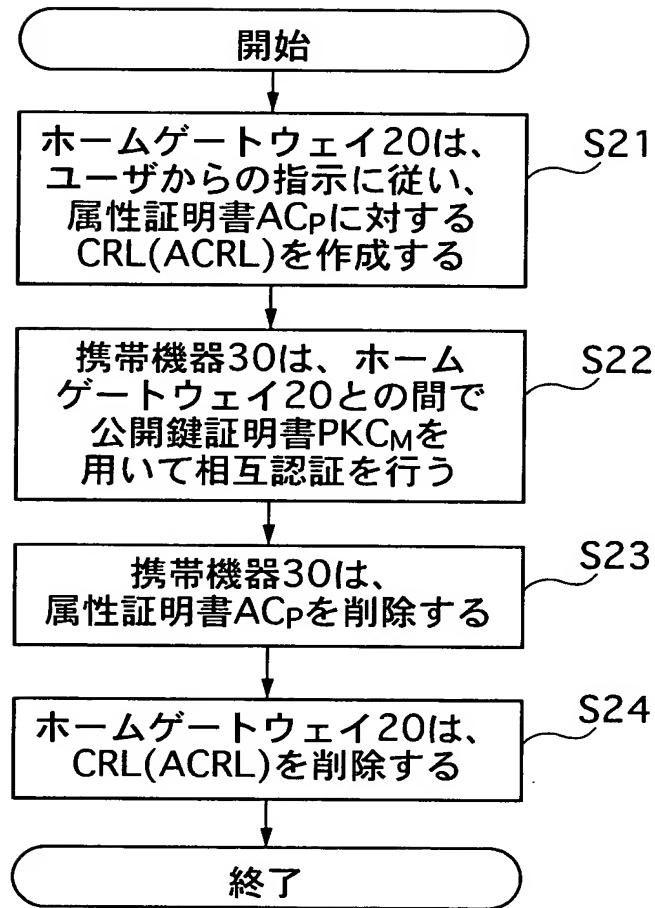
リモートアクセスシステムにおける一連の処理工程

【図 1 3】



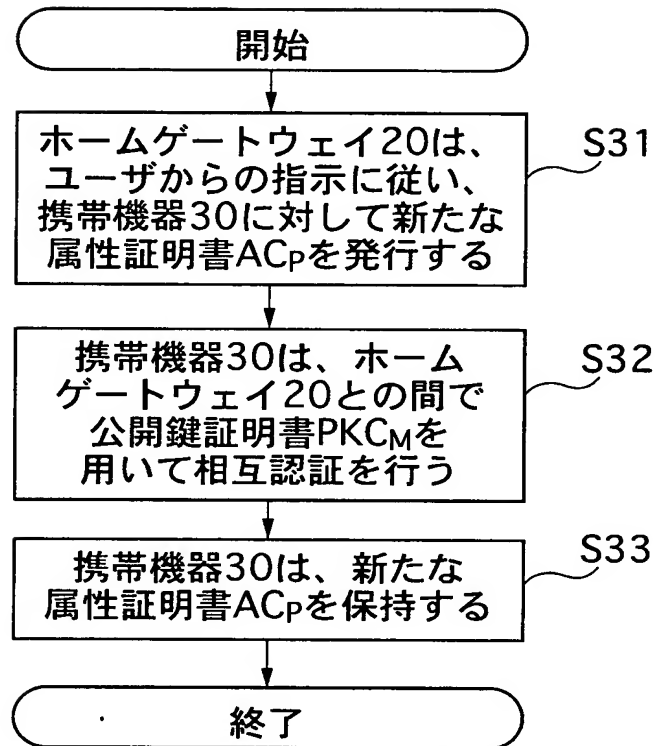
リモートアクセスシステムにおける一連の処理工程

【図 1 4】



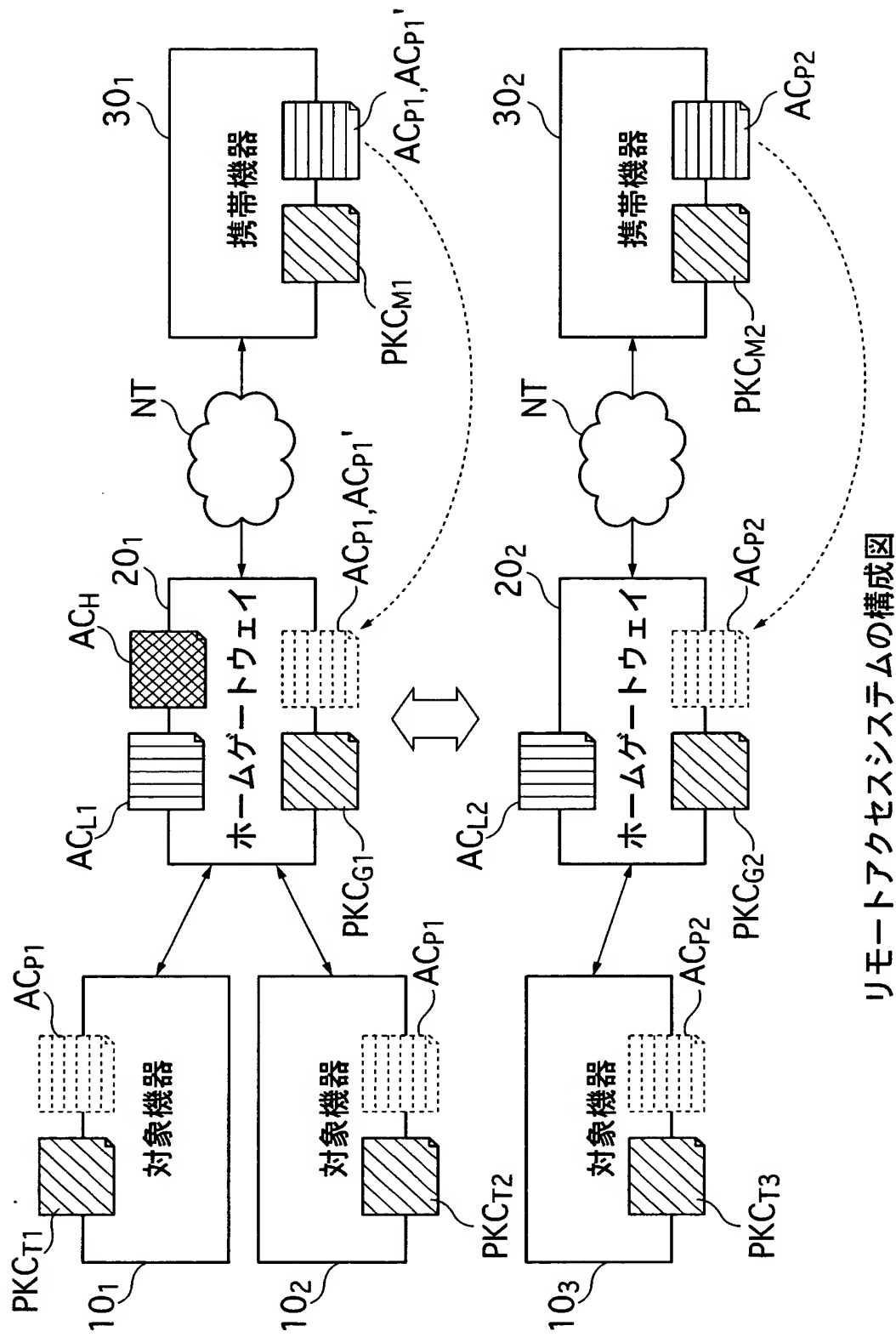
リモートアクセスシステムにおける一連の処理工程

【図 1 5】



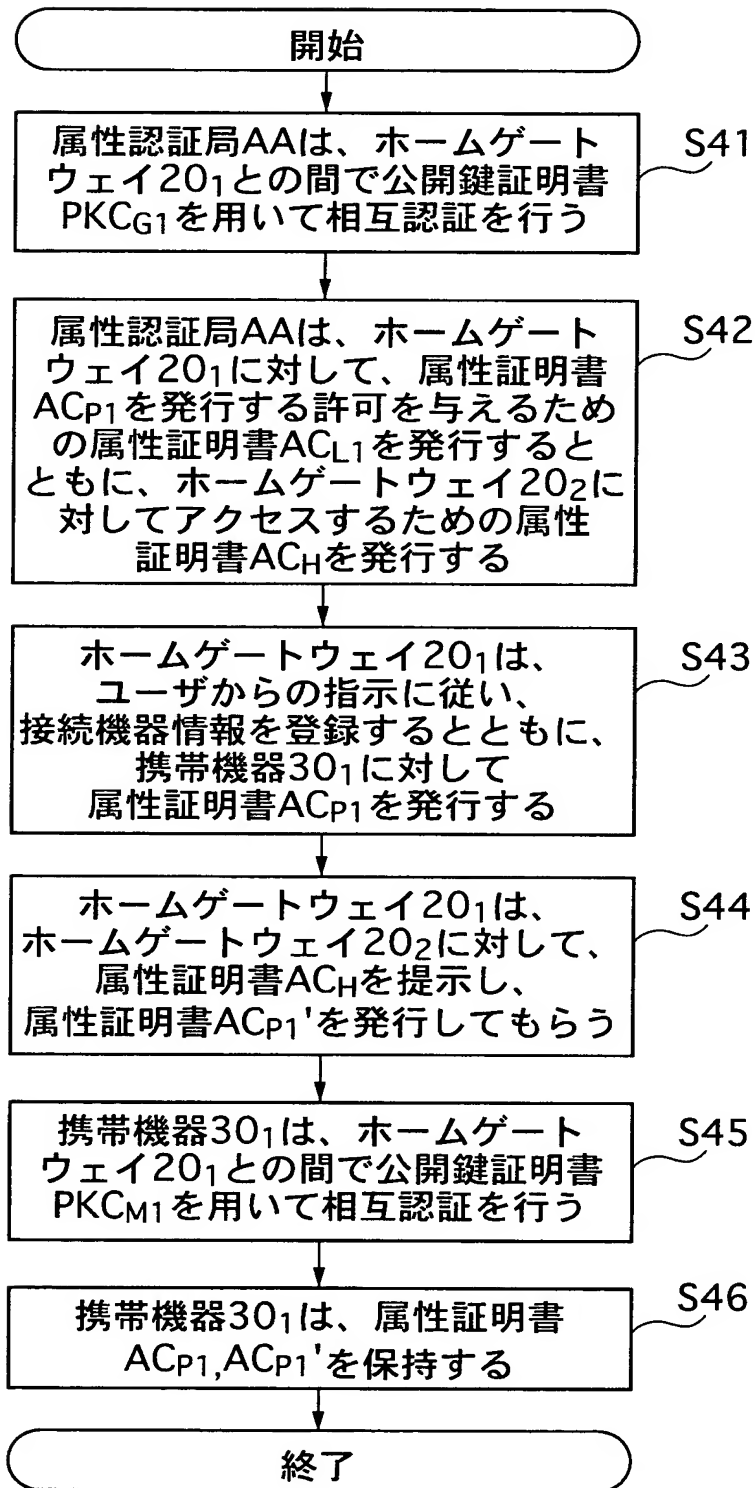
リモートアクセスシステムにおける一連の処理工程

【図16】



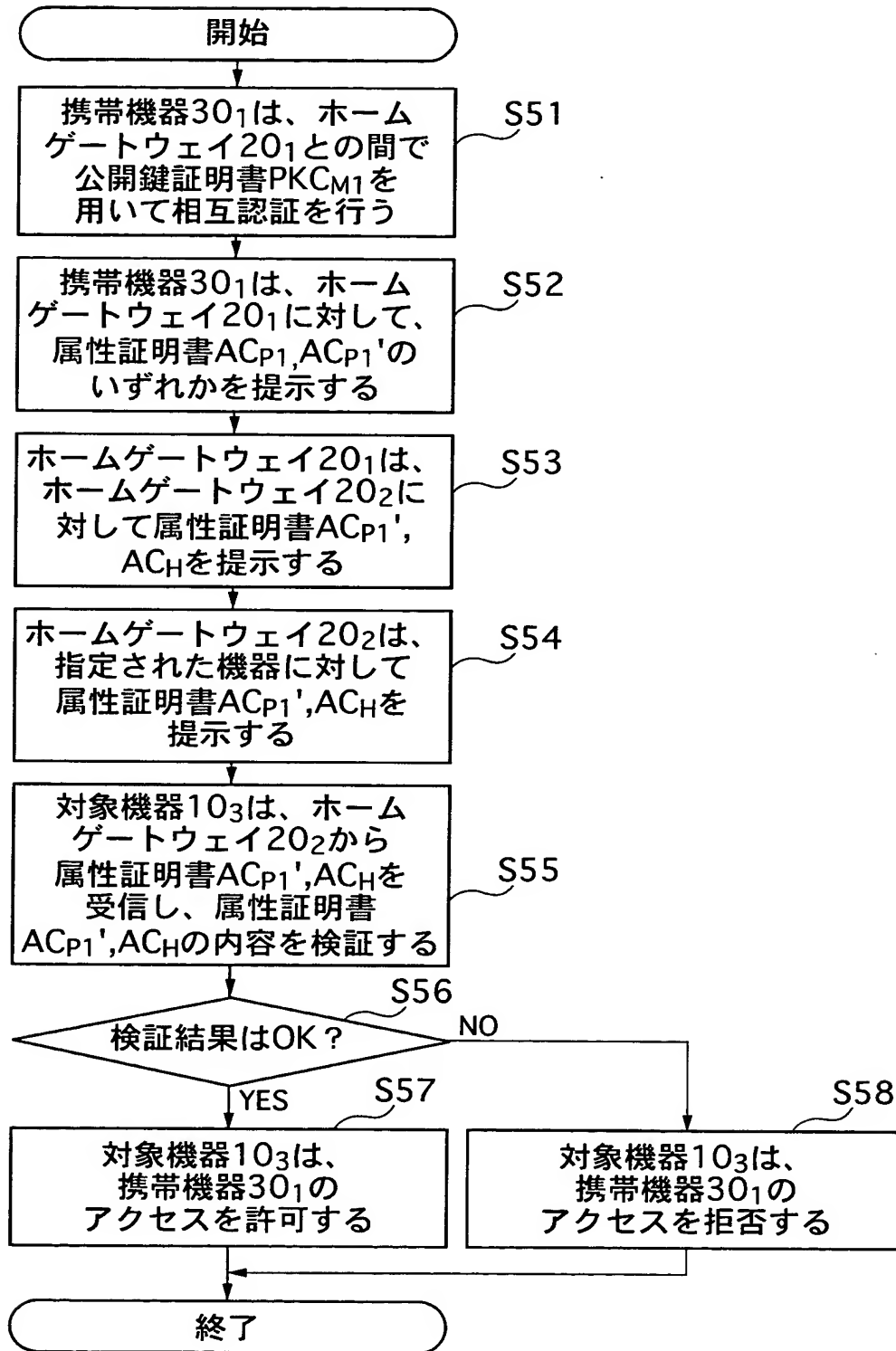
リモートアクセスシステムの構成図

【図 1 7】



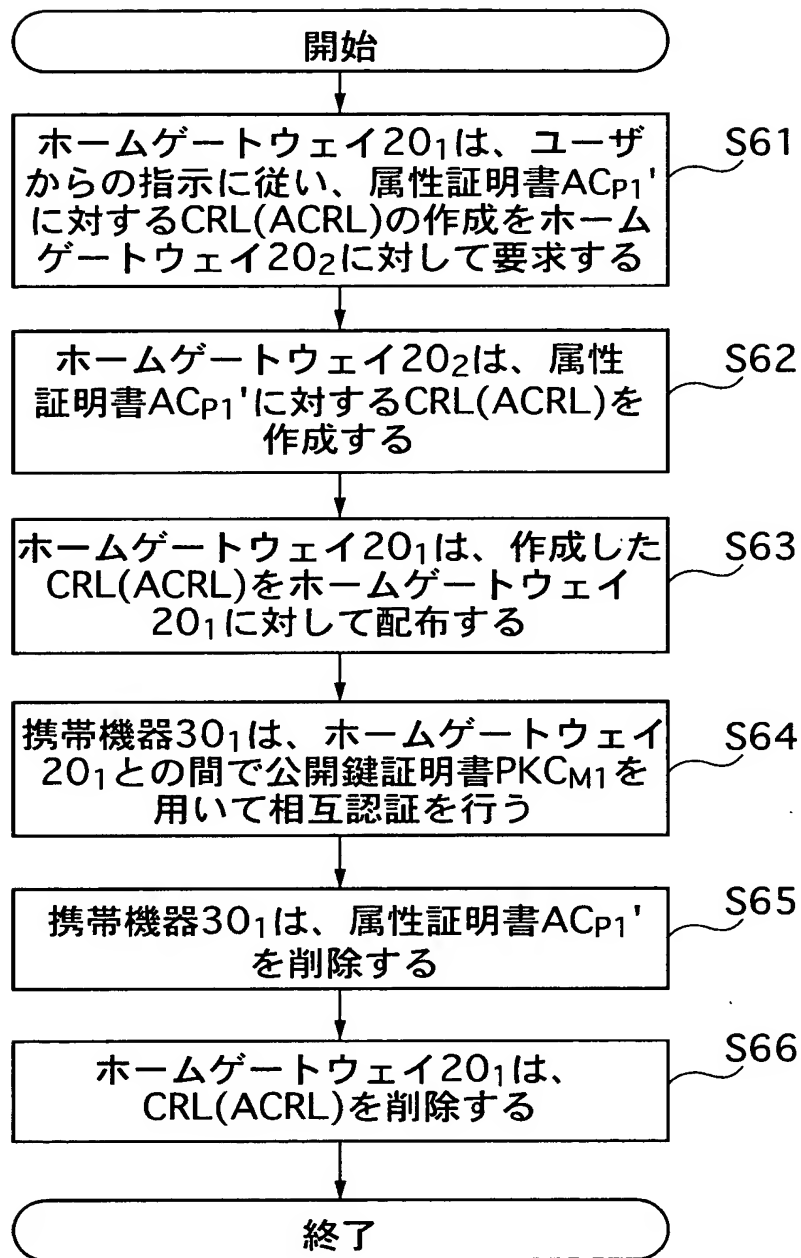
リモートアクセスシステムにおける一連の処理工程

【図 1 8】



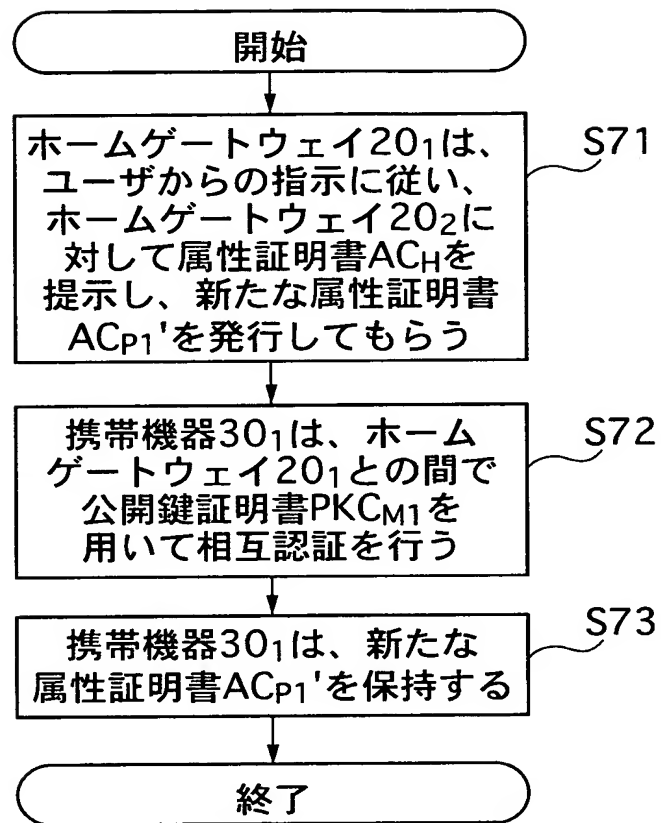
リモートアクセスシステムにおける一連の処理工程

【図 1 9】



リモートアクセスシステムにおける一連の処理工程

【図 2 0】



リモートアクセスシステムにおける一連の処理工程

【書類名】 要約書

【要約】

【課題】 リモートアクセスを行う際に、アクセスさせたいリソース毎に、権限単位での制御を容易且つ安全に行う。

【解決手段】 リモートアクセスシステムは、アクセスの対象となる対象機器 10₁, 10₂ と、これらの対象機器 10₁, 10₂ が属する家庭内ネットワークの入り口に相当する機器であるホームゲートウェイと 20 と、対象機器 10₁, 10₂ に対してアクセスするためにユーザが所持する携帯機器 30 とを、エンティティとして備える。リモートアクセスシステムにおいては、携帯機器 30 が、少なくともリソースに対する権限と経由させるホームゲートウェイ 20 の情報とが記述された属性証明書 AC_P を、ホームゲートウェイ 20 を介して対象機器 10₁, 10₂ に対して送信して提示することにより、リソースに対する携帯機器 30 のアクセスを検証する。

【選択図】 図 6

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社